InterSec/NQ30
V3.8

ユーザーズマニュアル

4 版

日本電気株式会社

目次

１．はじめに

１．１　コンポーネント構成

InterSec/NQ30a、InterSec/NQ30b、InterSec/NQ30c は、SecureVisor NetworkAgent をアプライアンス化したものです。SecureVisor は下記のコンポーネントから構成されます。

コンポーネント	説明
SecureVisor DomainManager	SiteManager からのデータを収集します。 収集したエージェントやホスト情報の管理方法により、以下の２つのモードがあります。 ■分散管理モード （従来どおり)SiteManager 毎に管理します。 ■集中管理モード DomainManager で統合管理します。
SecureVisor SiteManager	エージェントからのデータを収集し、DomainManager に転送します。 収集したエージェントやホスト情報の管理方法により、以下の3 つのモードがあります。 ■分散管理モード SiteManager 毎に管理します。 ■集中管理モード 「集中管理機能」を利用して DomainManager で統合管理します。 ■小規模管理モード 「集中管理機能」を利用して SiteManager 毎で管理します。
SecureVisor RemoteConsole	SiteManager の画面（サイトコンソール、ホスト一覧）を、リモートの PC から操作可能にします。
SecureVisor RemoteHosts	SiteManager の機能のうち、ホスト一覧のみをリモートの PC から操作可能にします。
SecureVisor NetworkAgent	ネットワーク上のパケットを監視してデータを生成し、SiteManager に通知します。
SecureVisor HostAgent	HostAgent インストールマシンの OS 種別やウイルスチェックソフトの情報を、NetworkAgent に通知します。
InterSec/NQ30a InterSec/NQ30b InterSec/NQ30c	SecureVisor NetworkAgent のアプライアンス版です。SecureVisor NetworkAgent とは設定方法などは異なりますが、一部機能を除き(※1)、基本機能に差異はありません。
SwitchManager	定期的にスイッチから情報を収集し、SiteManager に通知します。

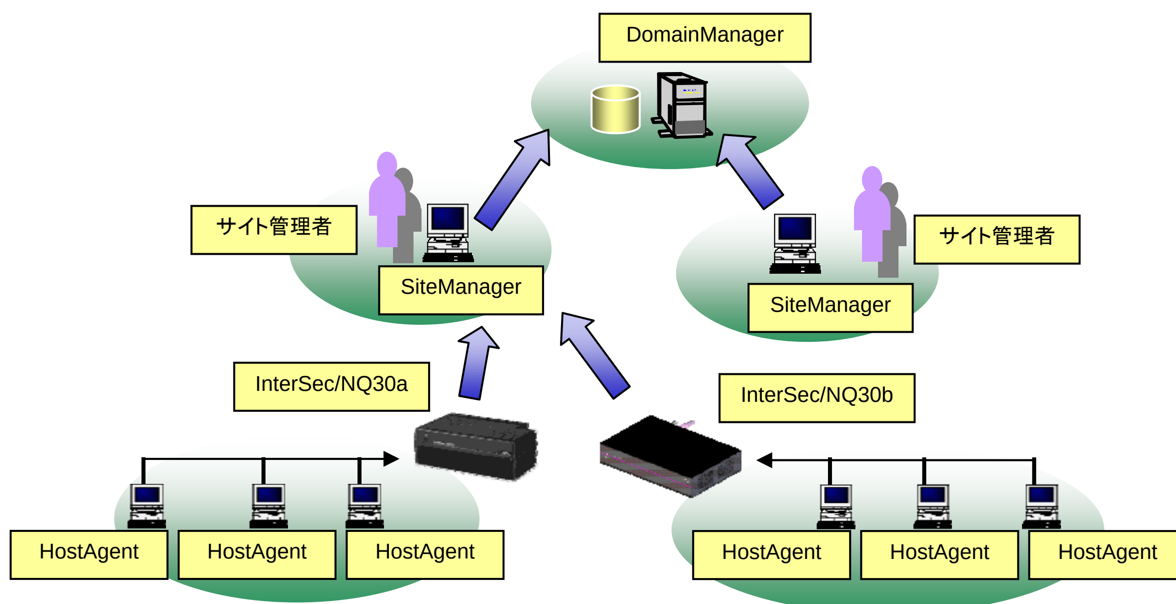
	また、NETCONF(※2)に対応しているスイッチの場合、不正端末が接続したポートの情報を取得することができます。

（※1） エージェントが NetworkAgent の場合、NQ 冗長化機能、承認申請機能は利用できません。
（※2） NETCONF(NETwork CONFiguration) ネットワーク機器を制御するための通信プロトコル。

本書では、このうち、InterSec/NQ30a、InterSec/NQ30b、InterSec/NQ30c のセットアップ手順、およびコマンドラインインターフェースについて説明します。SecureVisor Ver3.8 NetworkAgent の詳細は、SecureVisor Ver3.8 のマニュアル・ヘルプを参照してください。

１．２　各モジュールの相関図

各モジュールの相関図を以下に示します。



NQ は、各ネットワーク（＝IP サブネット＝ブロードキャストドメイン）に１台設置します。１台で約 2,000 件（NQ30c の場合は約 4,000 件）(※) のホスト情報を管理可能です。

また、SiteManager インストール PC 上から「共有ネットワーク対応機能」を設定する、あるいは USB メモリや telnet で「タグ VLAN 対応機能」を設定することで、１つの VLAN 内に複数のサブネットが存在する環境（共有ネットワーク環境）、複数 VLAN の環境、タグ VLAN（IEEE802.1Q）環境を１台の NQ で監視可能となります。「共有ネットワーク対応機能」の説明は１．５章、「タグ VLAN 対応機能」の説明は１．６章を参照してください。

（※）NetworkAgent が一日に検出した MAC アドレス数（目安としてホスト一覧の最終検出日がその日になっているものの件数）

１．３　用語説明

本書中の説明で使用する略語は、以下の通りです。

略語	意味
NQ30a	InterSec/NQ30a Ver3.8 を指します。文中にて左記の略語が指示された場合、InterSec/NQ30a Ver3.8 のみ該当します。
NQ30b	InterSec/NQ30b Ver3.8 を指します。文中にて左記の略語が指示された場合、InterSec/NQ30b Ver3.8 のみ該当します。
NQ30c	InterSec/NQ30c Ver3.8 を指します。文中にて左記の略語が指示された場合、InterSec/NQ30c Ver3.8 のみ該当します。
NQ	InterSec/NQ30a Ver3.8、InterSec/NQ30b Ver3.8、InterSec/NQ30c Ver3.8 を指します。文中にて左記の略語が指示された場合、InterSec/NQ30a Ver3.8、InterSec/NQ30b Ver3.8、InterSec/NQ30c 共通となります。
SiteManager	SecureVisor Ver3.8 SiteManager を指します。
DomainManager	SecureVisor Ver3.8 DomainManager を指します。

１．４　関連マニュアル

NQ の導入にあたり、以下のマニュアル類を参照してください。

「InterSec/NQ30a スタートアップガイド」(NQ30a ユーザの場合)
「InterSec/NQ30b スタートアップガイド」(NQ30b ユーザの場合)
「InterSec/NQ30c スタートアップガイド」(NQ30c ユーザの場合)
「SecureVisor Ver3.8 SiteManager インストールマニュアル」
「SecureVisor Ver3.8 DomainManager インストールマニュアル」
「SecureVisor Ver3.8 集中管理機能運用マニュアル」
「SecureVisor Ver3.8 注意制限事項」

※ バージョンアップを行った場合は、お手持ちのスタートアップガイドに記載されている設定手順と異なる場合がありますので、本書の各設定方法を確認してください。なお、バージョンアップ方法は、SiteManager オンラインヘルプの目次より、[SecureVisor]->[SecureVisor その他の機能]->[NetworkAgent 自動バージョンアップ機能]を参照してください。

１．５　共有ネットワーク環境での使用方法

NQ は通常、設定されたネットワークアドレスと同一のセグメントを監視対象としますが、「共有ネットワーク対応機能」を設定することにより、NQ が設置された環境に設定されたネットワークアドレスと異なるセグメントからのパケットが流れる場合も、監視対象とすることが可能となります。設定については、７．４章、または８．２章の「MultiNetwork」の項目を参照の上、USB メモリを使用した設定ファイルの反映や、telnet を介したネットワーク接続によるコマンド入力で行ってください。なお、「共有ネットワーク対応機能」を利用する場合、ネットワーク環境によって「InterSec/NQ30 1VLAN 追加ライセンス」の購入が必要となることがあります。以降の内容を確認し、必要に応じて追加ライセンスを購入してください。

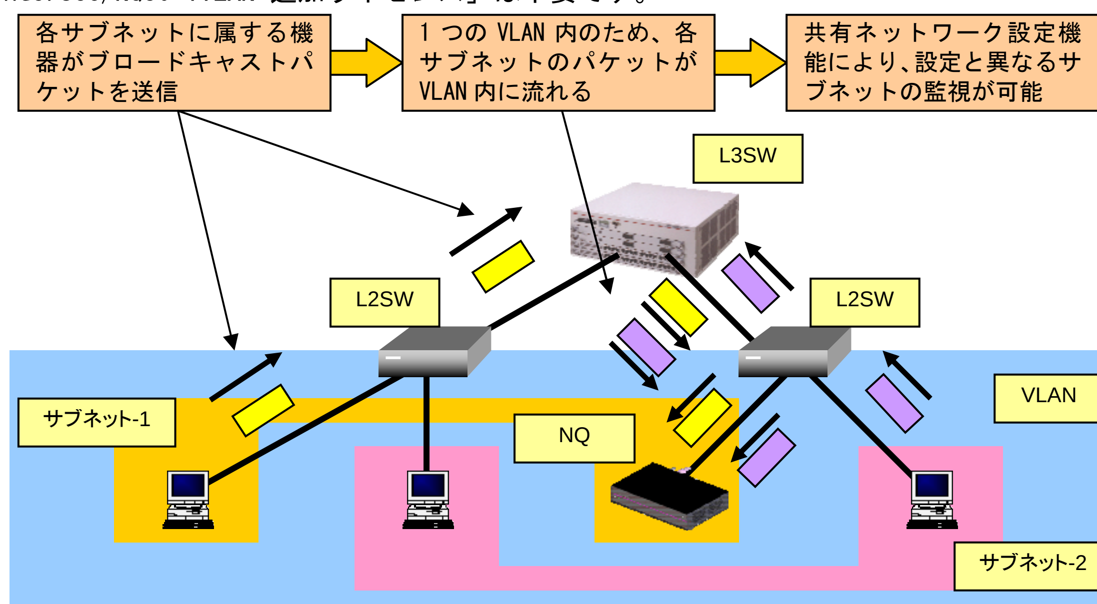
［本機能使用時の注意事項］

- 1 台の NQ で管理できるホスト台数は、2,000 件（NQ30c の場合は約 4,000 件）(※) までとなります。
- 「タグ VLAN 対応機能」との併用は未サポートです。
- InfoCage セキュリティリスク管理(CapsSuite)環境では、「共有ネットワーク対応機能」を使用することはできません。
- 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、サイトコンソールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないホストを防止することはできません。

（※）NetworkAgent が一日に検出した MAC アドレス数（目安としてホスト一覧の最終検出日がその日になっているものの件数）

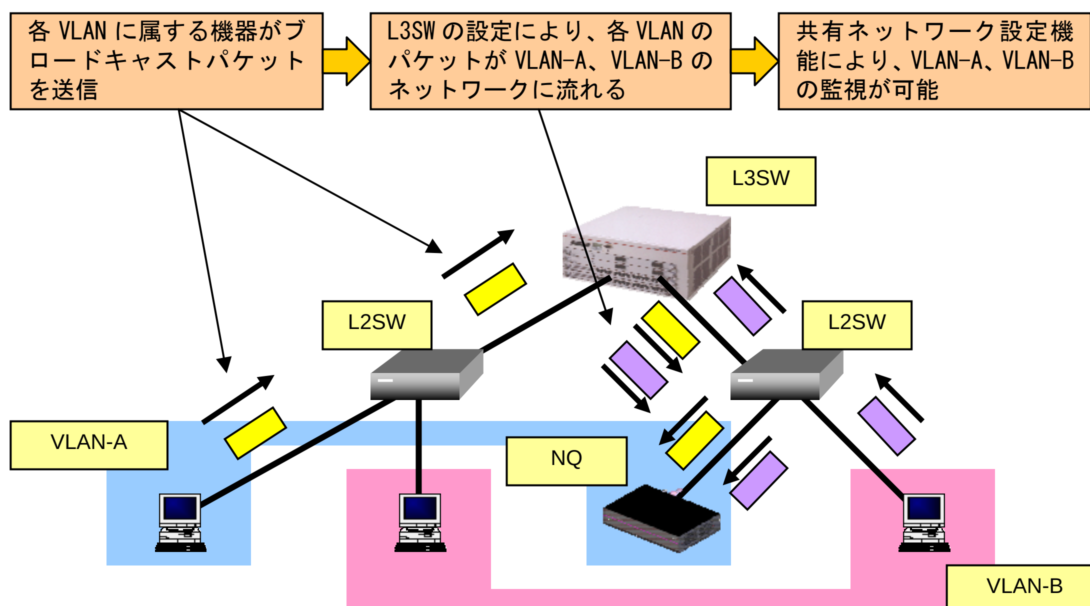
１．５．１　共有ネットワーク環境の場合

1 つの VLAN 内に複数のサブネットが存在する環境（共有ネットワーク環境）を監視する場合は、「InterSec/NQ30 1VLAN 追加ライセンス」は不要です。



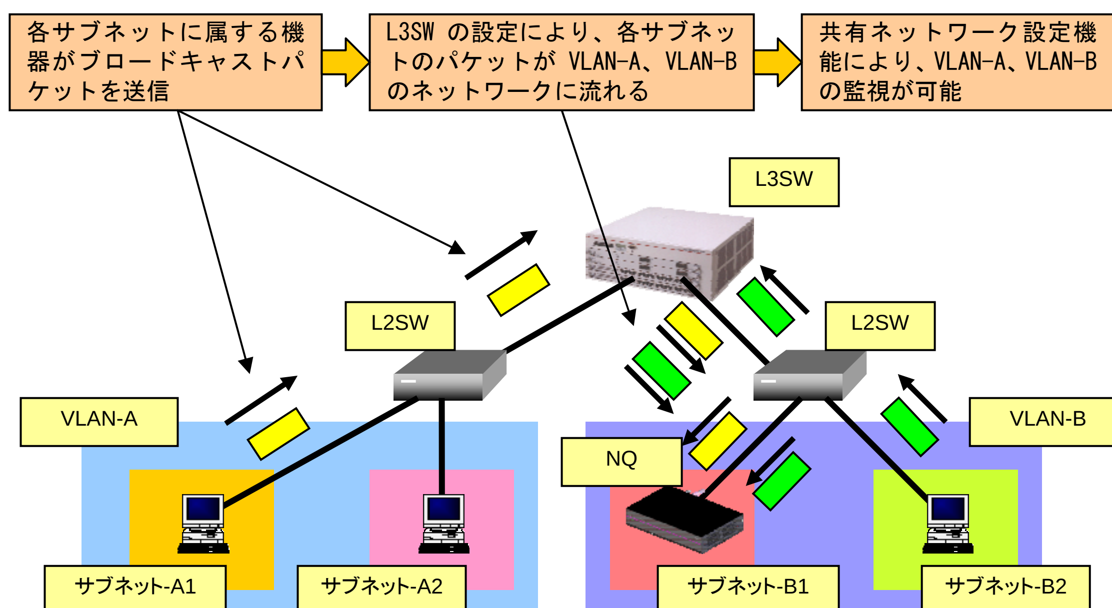
１．５．２　複数VLAN環境の場合

複数 VLAN の環境（非タグ VLAN 環境＝マルチ VLAN 環境）において、1 台の NetworkAgent（NQ）で複数の VLAN を監視する場合、“VLAN の数 － 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



１．５．３　共有ネットワーク＋複数VLAN環境の場合

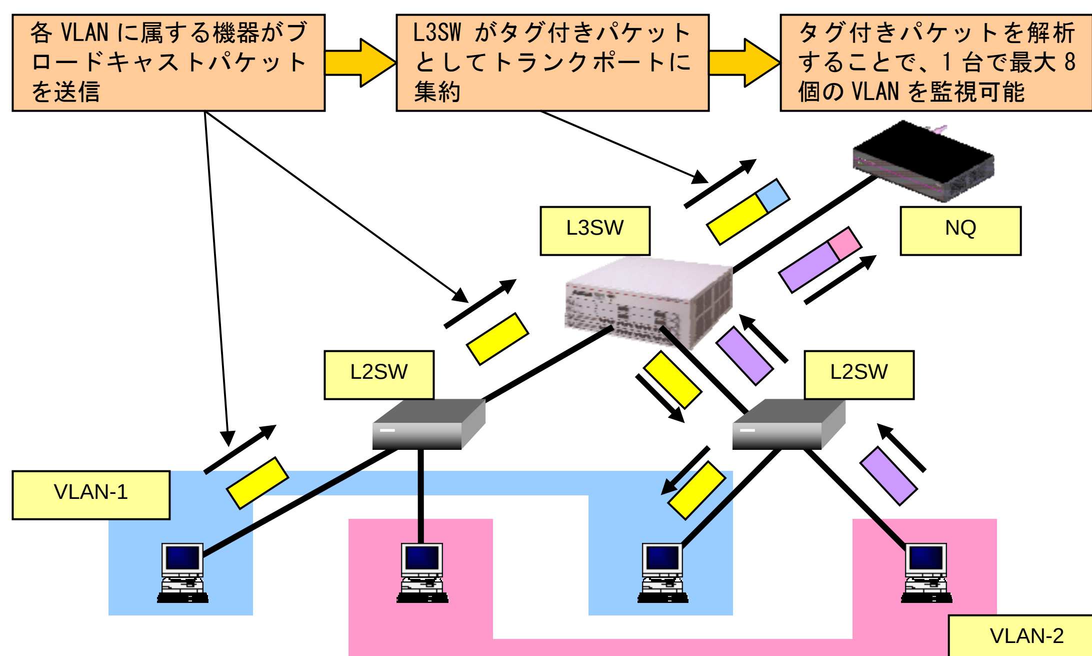
複数 VLAN（非タグ VLAN 環境＝マルチ VLAN 環境）で、各 VLAN 内に複数のサブネットが存在する環境を 1 台の NetworkAgent（NQ）で監視する場合、１．５．２章と同様に、“VLAN の数 － 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



１．６　タグVLAN（IEEE802.1Q）環境での使用方法

NQ は、タグ VLAN（IEEE802.1Q）環境[※1]での動作をサポートしています。L3 スイッチにタグ付きパケットの送受信を可能とするトランクポートを設定し、NQ をトランクポートに接続してデータ収集を行います。これにより、1 台の NQ で最大 8 個(NQ30c の場合、16 個)の VLAN を監視できます。設定については、２．２．４章のタグ VLAN 環境での設定パラメータ例、あるいは２．３．２章のタグ VLAN 環境設置時の実行例を参照の上、USB メモリを使用した設定ファイルの反映や、telnet を介したネットワーク接続によるコマンド入力で行ってください。

なお、タグ VLAN 環境において、1 台の NQ で複数の VLAN を監視する場合、“VLAN の数 – 1”の「InterSec/NQ30 1VLAN 追加ライセンス」が必要です。



[本機能使用時の注意事項]

- 1 台の NQ で管理できるホスト台数は、約 2,000 件（NQ30c の場合は約 4,000 件）[※2]までとなります。
- 「共有ネットワーク対応機能」との併用は未サポートです。
- 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、サイトコンソールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないホストを防止することはできません。
- NQ への telnet は、VLAN インターフェースで設定している IP アドレスに対して接続を行ってください。
- デフォルトゲートウェイの設定は、VLAN インターフェースに属するゲートウェイを指定してください。

(※1) サポート対象のタグ VLAN（IEEE802.1Q）環境は、IP サブネット ベース VLAN、ポート ベース VLAN です。

(※2) NetworkAgent が一日に検出した MAC アドレス数（目安としてホスト一覧の最終検出日がその日になっているものの件数）

１．７　共有ネットワーク＋タグVLAN（IEEE802.1Q）環境の場合

「共有ネットワーク対応機能」と「タグ VLAN 対応機能」の併用は未サポートです。１．５．３章、あるいは１．６章の使用方法で利用してください。

１．８　InterSec/NQ30b、NQ30cの初期化方法について

Ver3.6 から NQ30b の設定内容を初期化することが可能です。NQ30c はバージョンに関係なく初期化可能です。初期化内容は、パスワードやネットワーク情報など一部の情報を初期化する方法と、Ver3.1g（NQ30b の場合）、Ver2.2（NQ30c の場合）にダウングレードする方法があります。なお、NQ30a、および Ver3.6 未満の NQ30b では本機能は未サポートです。

１．８．１　初期化内容

初期化される内容は以下の通りです。

・パスワードやネットワーク情報などを初期化する場合

初期化内容	パラメータ	初期値
パスワード	Password	admin
IP アドレス	IpAddress	192.168.250.250
ネットワークマスク	NetworkMask	255.255.255.0
ネットワークアドレス	NetworkAddress	192.168.250.0
デフォルトゲートウェイアドレス	DefaultGateway	192.168.250.1
マネージャアドレス	ManagerIpAddress	192.168.250.251
ドメイン名	DomainName	isnq.dom
DNS サーバアドレス	DNSServer	未設定
エージェント名・ホスト名	AgentName	isnq30
タグ VLAN 設定情報	VLAN1～VLAN8 （NQ30c の場合は VLAN1～VLAN16）	未設定
通信速度	ifSpeed	auto
共有ネットワーク機能設定状態	MultiNetwork	Off
監視対象ネットワークリスト	NetworkList	未設定
不正接続防止設定状態	JamStatus	Off
データ収集設定状態	CollectOfPacket	Off
新規ホストの状態(色)	NewHostStatus	0

・ダウングレードして初期化する場合

NQ30b は Ver3.1g、NQ30c は Ver2.2 へダウングレードし、「パスワードやネットワーク情報などを初期化する場合」の内容に加え、以下のエージェント設定の項目も初期化されます。

初期化内容	パラメータ	初期値
設置場所	AgentLocation	未設定
管理者氏名	AdminName	未設定
管理者電話番号	AdminTelephoneNumber	未設定
管理者メールアドレス	AdminMailAddress	未設定
マネージャポート	ManagerPort	23490
DHCP スコープ	DhcpScope	未設定

１．８．２　初期化方法

NQ30b、NQ30c の電源を投入した直後から STATUS ランプが橙に点灯するまでの間 STATUS スイッチ(※) を押下し続けると初期化を行います。

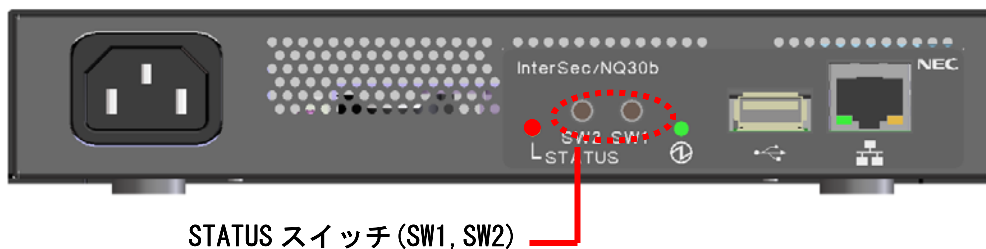
初期化内容	使用する STATUS スイッチ
パスワードやネットワーク情報などを初期化する場合	SW1
ダウングレードして初期化する場合	SW1 と SW2

STATUS ランプが赤に点灯すると初期化が完了します。その後、NetworkAgent サービスを起動し、定常状態になると、STATUS ランプは緑色に点灯します。

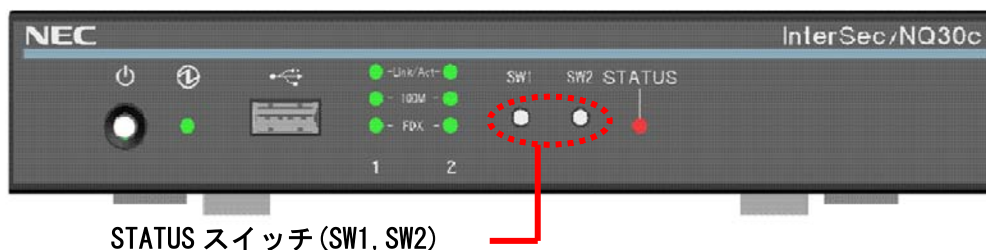
※ダウングレード中に電源断などにより初期化が失敗した場合、次の NQ 起動時に再度初期化を行います。

(※)NQ30b、NQ30c の STATUS スイッチ

■NQ30b 背面パネルイメージ



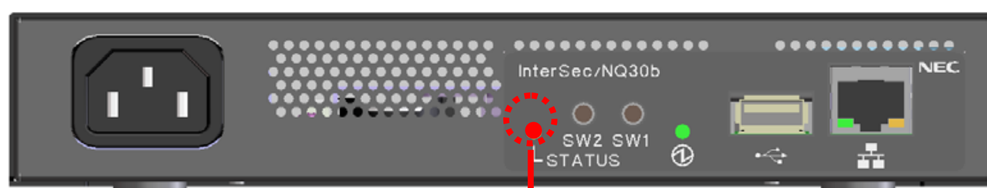
■NQ30c 前面パネルイメージ



１．９　InterSec/NQ30b、NQ30cの動作状況確認方法について

Ver3.6 から NQ30b、NQ30c の STATUS ランプで NetworkAgent、OS の動作状況を確認することが可能となりました。STATUS ランプは、NQ30c は前面と背面、NQ30b は背面にあります。なお、工場出荷時の NQ30b および、NQ30a では本機能は未サポートです。

■NQ30b 背面パネルイメージ



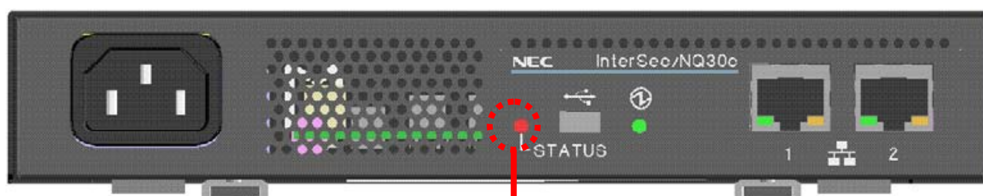
STATUS ランプ

■NQ30c 前面パネルイメージ



STATUS ランプ

■NQ30c 背面パネルイメージ



STATUS ランプ

STATUS ランプの状態	InterSec/NQ30b、NQ30c の状態
消灯	電源 OFF の状態
赤の点灯	OS 起動中で NetworkAgent サービス停止中の状態
緑の点灯	OS、NetworkAgent サービス起動中の状態(定常状態)
橙の点灯	自動バージョンアップ中または、STATUS ボタン押下による初期化中の状態 ※ この状態で電源 OFF しないでください。

例１） 電源投入時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b、NQ30c の状態
消灯	電源 OFF の状態
赤の点灯	電源 ON し、OS を起動
緑の点灯	NetworkAgent サービスを起動し、定常状態

例２）自動バージョンアップ時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b、NQ30c の状態
緑の点灯	定常状態
赤の点灯	SiteManager よりバージョンアップモジュールをダウンロードし、NetworkAgent サービスを停止
橙の点灯	バージョンアップ中
消灯	バージョンアップ完了後、本体をリブートするため一旦、電源 OFF
赤の点灯	電源 ON され、OS を起動
緑の点灯	NetworkAgent サービスを起動し、定常状態に戻る

例３）STATUS ボタン押下による初期化時の STATUS ランプの状態遷移

STATUS ランプの状態	InterSec/NQ30b、NQ30c の状態
消灯	電源 OFF の状態
赤の点灯	電源 ON し、OS を起動
橙の点灯	STATUS ボタン押下による初期化処理中
赤の点灯	初期化処理完了
緑の点灯	NetworkAgent サービスを起動し、定常状態に戻る

２．セットアップ

工場出荷時の NQ は以下の通り、暫定的なバージョンの NetworkAgent がプリインストールされています。

製品名	製品型番	バージョン
InterSec/NQ30a	N8100-1110Q	2.2g
InterSec/NQ30b	N8100-1200Q	2.2h
	N8100-1300Q	3.1g
InterSec/NQ30c	N8100-1400Q	2.2-3.8(※)

（※）バージョン 2.2 から 3.8 に対応するモジュールがプリインストールされています。

従いまして、初期導入時に下記の手順によるバージョンアップ手続きが必要です。なお、バージョンアップについての説明、注意事項に関しては、SiteManager オンラインヘルプの、[SecureVisor]->[SecureVisor その他の機能]->[NetworkAgent 自動バージョンアップ機能]を参照してください。Ver3.7 より SiteManager のバージョンアップ後、特定の NQ のみ手動で更新することも可能です。

【InterSec/NQ30a、InterSec/NQ30b の場合】

① NQ に対して、SiteManager と通信するために必要な初期設定(７．１章を参照)を行い、ネットワークに接続する。

② NQ が SiteManager へ接続し、自動更新を行う(SiteManager から Ver3.8 の内部ソフトウェアをダウンロードし、インストールを自動的に行います)。

③ Ver3.8にバージョンアップ後､Ver3.8に対する必要な設定を行う｡承認申請機能の利用､Apple社製端末やLinux系OS端末、携帯端末を監視対象に含める場合に設定が必要なパラメータがあります。設定するパラメータは必要に応じて下記章を参照してください。
- ・７．４　各環境共通の設定可能パラメータ
- ・８．２　確認、および変更が可能な属性の詳細
- ・９．６　Apple社製端末を監視対象にする場合の設定必須パラメータ
- ・９．７　Linux系OS端末を監視対象にする場合の設定必須パラメータ
- ・９．８　携帯端末を監視対象にする場合の設定必須パラメータ

④ 運用開始する。

なお、バージョンアップについての説明、注意事項に関しては、SiteManager オンラインヘルプの [SecureVisor]－[SecureVisor その他の機能]－[NetworkAgent 自動バージョンアップ機能]を参照してください。

【InterSec/NQ30c の場合】
工場出荷時にバージョン 2.2 から 3.8 に対応するモジュールがプリインストールされています。よって、バージョン 3.8 として使用する場合、バージョンアップは不要です。

① SiteManagerと通信するために必要な初期設定とVer3.8 に対する必要な設定を行い、ネットワークに接続する。承認申請機能の利用、Apple社製端末やLinuxOS、携帯端末を監視対象に含める場合に設定が必要なパラメータがあります。設定するパラメータは必要に応じて下記章を参照してください。
- ７．４　各環境共通の設定可能パラメータ
- ８．２　確認、および変更が可能な属性の詳細
- ９．６　Apple社製端末を監視対象にする場合の設定必須パラメータ
- ９．７　Linux系OS端末を監視対象にする場合の設定必須パラメータ

２．１　セットアップ方法

NQ のセットアップは、以下の 2 つの方法があります。

- USB メモリを使用して設定ファイルを反映させる　→　２．２章参照
- telnet を介したネットワーク接続によりコマンドを入力する　→　２．３章参照

２．２　USBメモリを使用したセットアップ

２．２．１　USBメモリを使用したセットアップ手順

USB メモリを使用したセットアップ手順は以下の通りです。

① SiteManager をインストールする

「SecureVisor Ver3.8 SiteManager インストールマニュアル」を参照し、管理サーバに SiteManager をインストールしてください。

② USB メモリに設定ファイルを作成する

USB メモリのルートフォルダに設定ファイルを作成してください。設定ファイルの作成方法は、２．２．２章～２．２．４章を参照してください。NQ は、USB メモリのルートフォルダに保存された設定ファイルのみ認識することができます。

③ USB メモリを差込み、NQ を起動する

NQ 筐体へ設定ファイルを保存した USB メモリ､ネットワークに接続された LAN ケーブル、電源ケーブルを接続してください。接続完了後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。

【注意事項】
・NQ30c の背面パネルにある mini USB ポートは使用できません。
・NQ30c は USB2.0 の USB メモリのみ使用できます。
・USB メモリから設定ファイルを認識させることができるのは、起動時のみです。NQ の起動後に筐体へ USB メモリを接続しても､設定ファイルを認識させることはできませんので注意してください。
・NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

④ USB メモリの認識状態を確認する

NQ が USB メモリを正常に認識したことを確認するため、起動から約 1 分経過後、NQ 筐体から USB メモリを取り外し、USB メモリを PC に接続してください。NQ が USB メモリを正常に認識できた場合は､USB メモリのルートフォルダにテキストファイル(svconflog.txt)が作成されます。テキストファイルが作成されない場合､NQ と USB メモリの相性が悪い、NQ が暗号化 USB メモリに対応していないなどが原因で、認識できていない可能性があります。テキストファイルの詳細は、６．２章を参照してください。

⑤ パスワードの認証結果を確認する

NQ が USB メモリ内の設定ファイルから認証パスワードを確認する際に認証エラーとなった場合、④で作成されたテキストファイルにエラーログが出力されます。エラーログが出

力された場合は２．２．２章を参照し、設定ファイルの記述フォーマットに問題がないか確認してください。また、７．１章の「Password」の項目を参照し、認証パスワードの記述方法に問題がないか確認してください。なお、エラーログの詳細は、６．２章を参照してください。

⑥ パラメータの設定状況を確認する

NQ が USB メモリ内の設定ファイルから実行したパラメータの設定状況は、パスワードの認証結果と同様、④で作成されたテキストファイルに出力されます。エラーログが出力された場合は２．２．２章、３．６章を参照し、設定ファイルの記述フォーマット、パラメータ、設定値に問題がないか、確認してください。

設定ファイルの例とログの出力イメージは以下の通りです。

[設定ファイル]

```
password:admin
MultiNetwork:On
DisablePreventionAutoIPAddr:On
```

[出力イメージ]

```
2009/12/04 14:07:55 JST: mount ok
+ Welcome to SvNaConsole.
set if auto on
+ Command succeeded.
set na MultiNetwork On
+ Command succeeded.
set na DisablePreventionAutoIPAddr On
+ Command succeeded.
+ Goodbye.
```

⑦ NQ の設定状態を確認する

NQ の起動時に、設定ファイルで接続先として指定した SiteManager インストール PC と正常に通信可能で、SiteManager サービスが起動している場合は、設定ファイルにて指定したエージェント名のアイコンが SiteManager インストール PC 上のサイトコンソールに表示されます。

サイトコンソールに表示されない場合や SiteManager サービスが起動していない場合は、６．３章を参照して NQ の設定状態を確認してください。

⑧ VLAN インターフェースの設定状態を確認する

非タグ VLAN 環境で使用する場合、VLAN インターフェースが設定されていると、正常にデータ収集ができません。ネットワークインターフェース確認コマンド（３．６．３章参照）

で設定状態を確認し、VLAN インターフェースが設定されていれば７．４章の「Vlan(-)」の項目、または VLAN インターフェース削除コマンド（３．６．２１章参照）を参照の上、USB メモリを使用した設定ファイルの反映や、telnet を介したネットワーク接続によるコマンド入力で設定の削除を行ってください。
タグ VLAN 環境で使用する場合、VLAN インターフェースの設定数は、最大で 8 個（NQ30c の場合は 16 個）までのサポートとなります。不要な VLAN インターフェースが設定されている場合、削除して使用してください。

２．２．２　設定ファイル作成方法

［ファイル名］

svconfig.txt　（全て半角小文字）

［注意事項］

・設定ファイルで使用可能な文字コードは、Shift_JIS、および日本語EUC(EUC-JP)です。また、使用可能な改行コードは、<CR>+<LF>、および<LF>です。使用するテキストエディタの設定を確認の上、作成してください。なお、Windows 標準のメモ帳は Shift_JIS、<CR>+<LF>で作成されます。設定ファイルの文字コードに日本語 EUC を使用する場合、設定ファイル内での文字コード指定が必須となります。
・設定ファイルは、同一のパラメータを複数行記述しないでください。同一パラメータが複数行記述されている場合、後に記述されたパラメータの内容が設定されます。
・設定ファイルは、1行につき1個のパラメータを記述してください。複数のパラメータを記述する場合は、改行してください。
・パラメータと設定値の間は、コロン（:）で区切ってください。
・パラメータと設定値は、1行で記述してください。記述行には、不要な改行や半角スペースなどを記述しないでください。
・設定必須パラメータは、パラメータに対する設定値を必ず設定してください。
・設定可能パラメータは、設定値がなければ設定ファイルへ記述しないでください。
・設定ファイルへ設定パラメータを記述しない場合、設定済の値（工場出荷時は既定値）が使用されます。
・設定ファイル内に、設定削除のパラメータと設定反映のパラメータを記述する場合、設定削除パラメータ以降に設定反映パラメータを記述してください。設定削除のパラメータは、パラメータの末尾に「(-)」が記述されたものが該当します。
・設定ファイルは、最後のパラメータ記述後、改行してください。

［設定項目］

設定ファイルの記述例は、非タグ VLAN 環境への初期設定時は２．２．３章、タグ VLAN 環境への初期設定時は２．２．４章を参照してください。設定パラメータの詳細は、７章を参照してください。記述例に記述されていない設定可能パラメータは、必要に応じて設定ファイルに追記して使用してください。

２．２．３　非タグVLAN環境への初期設定時の設定パラメータ例

以下に非タグ VLAN 環境へ導入する際の初期設定例を示します。設定パラメータを変更、または追記する場合、７章を参照して適切な設定を記述してください。

［設定例］

設定	説明
Password:admin	認証パスワード
AgentName:isnq30	エージェント名
IpAddress:192.168.250.250	エージェントの IP アドレス
NetworkMask:255.255.255.0	サブネットマスク
ManagerAddress:192.168.250.249	サイトマネージャアドレス
DNSServer:192.168.250.2 192.168.250.3	DNS サーバアドレス
DomainName:isnq.dom	ドメイン名
DefaultGateway:192.168.250.1	デフォルトゲートウェイアドレス

２．２．４　タグVLAN環境への初期設定時の設定パラメータ例

以下にタグ VLAN 環境へ導入する際の初期設定例を示します。設定パラメータを変更、または追記する場合、７章を参照して適切な設定を記述してください。

［設定例］

Password:admin	認証パスワード
AgentName:isnq30	エージェント名
IpAddress:127.0.0.1	NQ の IP アドレス
ManagerAddress:192.168.250.249	サイトマネージャアドレス
Vlan1:192.168.10.250 24 111	VLAN ID 111 の設定
Vlan2:192.168.20.250 24 112	VLAN ID 112 の設定
Vlan3:192.168.30.250 24 113	VLAN ID 113 の設定
Vlan4:192.168.40.250 24 114	VLAN ID 114 の設定
Vlan5:192.168.50.250 24 115	VLAN ID 115 の設定
Vlan6:192.168.60.250 24 116	VLAN ID 116 の設定
Vlan7:192.168.70.250 24 117	VLAN ID 117 の設定
Vlan8:192.168.80.250 24 118	VLAN ID 118 の設定
DNSServer:192.168.10.2 192.168.10.3	DNS サーバアドレス
DomainName:isnq.dom	ドメイン名
DefaultGateway:192.168.10.254	デフォルトゲートウェイアドレス

２．３　ネットワーク接続を使用したセットアップ

２．３．１　ネットワーク接続を使用したセットアップ手順

telnet を介したネットワーク接続を使用したセットアップ手順は以下の通りです。

① SiteManager をインストールする

「SecureVisor Ver3.8 SiteManager インストールマニュアル」を参照し、管理サーバに SiteManager をインストールしてください。

② NQ を起動する

NQ 筐体へ、ネットワークに接続された LAN ケーブル (※)、電源ケーブルを接続してください。接続完了後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

（※）タグ VLAN 環境で使用する場合、工場出荷時の状態では L3SW のタグ付きパケットの送受信を可能とするトランクポートに接続しても通信できません。非タグ VLAN 環境に接続して設定を行い、NQ の再起動後、トランクポートに接続してください。

③ telnet クライアント PC を用意する

NQ の初期ネットワーク設定は以下の通りです。

IP アドレス	: 192.168.250.250
サブネットマスク	: 255.255.255.0
デフォルトゲートウェイアドレス	: 192.168.250.1
DNS サーバアドレス	: 設定なし

PC に NQ と同じネットワークの IP アドレス(例えば 192.168.250.111)を設定し、NQ と同じ LAN に接続してください。接続後、ping コマンドなどを使用して NQ との通信状態を確認してください。

［実行例］

```
C:¥> ping 192.168.250.250 (※)
```

(※)斜体部分は、NQ に設定されている IP アドレス、あるいは IP アドレスに割り当てられているホスト名を設定してください。実行例の IP アドレスは、工場出荷時の設定です。

NQ と通信できない場合は、NQ に設定されているネットワークと接続できるよう、telnet クライアント PC のネットワーク設定を確認してください。

④ ネットワーク接続を使用してセットアップする

telnet クライアント PC で、telnet を介して NQ に接続し、セットアップを行ってください。Windows PC のコマンドプロンプトを使用したセットアップ方法の例を２．３．２章に記載していますので確認してください。セットアップ完了後は、設定内容を反映させるため、必ず NQ の再起動を行ってください。なお、各コマンドの詳細は、３章、８章を参照してください。

⑤ NQ の設定状態を確認する

NQ の起動時に、接続先として設定した SiteManager インストール PC と正常に通信可能で、SiteManager サービスが起動している場合は、NQ に設定されているエージェント名のアイコンが SiteManager インストール PC 上のサイトコンソールに表示されます。

サイトコンソールに表示されない場合や SiteManager サービスが起動していない場合は、６．３章を参照して NQ の設定状態を確認してください。

２．３．２　ネットワーク接続を使用したセットアップの実行例

［注意］

・設定しない属性については、該当のコマンドを実行する必要はありません。

・非タグ VLAN 環境で使用する場合、VLAN インターフェースが設定されていると、正常にデータ収集ができません。ネットワークインターフェース確認コマンド（３．６．３章参照）で設定状態を確認し、VLAN インターフェースが設定されていれば７．４章の「Vlan(-)」の項目、または VLAN インターフェース削除コマンド（３．６．２１章参照）を参照の上、USB メモリを使用した設定ファイルの反映や、telnet を介したネットワーク接続によるコマンド入力で設定の削除を行ってください。

・タグ VLAN 環境で使用する場合、VLAN インターフェースの設定数は、最大で 8 個（NQ30c の場合は 16 個）までのサポートとなります。不要な VLAN インターフェースが設定されている場合、削除して使用してください。

［実行例］

■非タグ VLAN 環境設置時の実行例

```
C:¥>telnet 192.168.250.250 23496
- 400 require authentication
svna> pass admin
+ Welcome to SvNaConsole.
svna> set us admin xxxxxxxx
+ Command succeeded.
svna> set if auto off
+ Command succeeded.
svna> set ns nameserver 10.1.2.6 10.1.2.7
+ Command succeeded.
svna> set ns domain isnq30.dom
+ Command succeeded.
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:172.16.171.255
        UP  BROCAST  RUNNING  MULTICAST
eth0.100        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.10.255
        Default Gateway:192.168.10.254
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove vlan eth0.100
+ Command Succeeded.
svna> set if eth0 address 10.1.2.252 mask 255.255.255.0
+ Command succeeded.
svna> set gw 10.1.2.254
+ Command succeeded.
svna> set na stop
+ Command succeeded.
svna> set hn isnq30
+ Command succeeded.
svna> set sm 10.1.2.253
+ Command succeeded.
svna> reboot
 + Command succeeded.
```

→ telnet によるネットワーク接続の詳細は３．２章参照

→ 認証コマンドの詳細は３．６．１章参照

→ パスワード変更コマンドの詳細は３．６．２章参照

→ ネットワークインターフェース設定の反映タイミング変更コマンドの詳細は３．６．６章参照

→ DNS サーバアドレス設定コマンドの詳細は３．６．９章参照

→ ドメイン名設定コマンドの詳細は３．６．１０章参照

→ネットワークインターフェース確認コマンドの詳細は３．６．３章参照

→VLAN インターフェースが設定されている場合、必ず削除してください
なお、工場出荷時は実行不要です

→VLAN インターフェース削除コマンドの詳細は３．６．２１章参照

→ ネットワークインターフェース設定コマンドの詳細は３．６．７章参照

→ デフォルトゲートウェイアドレス設定コマンドの詳細は３．６．２２章参照

→ エージェント停止コマンドの詳細は３．６．２５章参照

→ エージェント名設定コマンドの詳細は３．６．１５章参照

→ マネージャ設定コマンドの詳細は３．６．１４章参照

→ 再起動コマンドの詳細は３．６．１３章参照

■タグ VLAN 環境設置時の実行例

```
C:¥>telnet 192.168.250.250 23496
- 400 require authentication
svna> pass admin
+ Welcome to SvNaConsole.
svna> set us admin xxxxxxxx
+ Command succeeded.
svna> set if auto off
+ Command succeeded.
svna> set ns nameserver 10.1.2.6 10.1.2.7
+ Command succeeded.
svna> set ns domain isnq30.dom
+ Command succeeded.
svna> list if
= Command succeeded.
eth0     inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
         Mask:255.255.255.0  Bcast:172.16.171.255
         UP  BROCAST  RUNNING  MULTICAST
eth0.100        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
         Mask:255.255.255.0  Bcast:192.168.10.255
         Default Gateway:192.168.10.254
         UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove vlan eth0.100
+ Command Succeeded.
svna> add vlan eth0 111
+ Command succeeded.
svna> set if eth0.111 address 10.1.2.252 mask 255.255.255.0
+ Command succeeded.
svna> set if eth0 address 127.0.0.1
+ Command succeeded.
svna> set gw 10.1.2.254
+ Command succeeded.
svna> set na stop
+ Command succeeded.
svna> set hn isnq30
+ Command succeeded.
svna> set sm 10.1.2.253
+ Command succeeded.
svna> reboot
 + Command succeeded.
```

→ telnet によるネットワーク接続の詳細は３．２章参照

→ 認証コマンドの詳細は３．６．１章参照

→ パスワード変更コマンドの詳細は３．６．２章参照

→ ネットワークインターフェース設定の反映タイミング変更コマンドの詳細は３．６．６章参照

→ DNS サーバアドレス設定コマンドの詳細は３．６．９章参照

→ ドメイン名設定コマンドの詳細は３．６．１０章参照

→ネットワークインターフェース確認コマンドの詳細は３．６．３章参照

→不要な VLAN インターフェースが設定されている場合、削除してください
なお、工場出荷時は実行不要です

→VLAN インターフェース削除コマンドの詳細は３．６．２１章参照

→ VLAN インターフェース追加コマンドの詳細は３．６．２０章参照

→ ネットワークインターフェース設定コマンドの詳細は３．６．７章参照

→ デフォルトゲートウェイアドレス設定コマンドの詳細は３．６．２２章参照

→ エージェント停止コマンドの詳細は３．６．２５章参照

→ エージェント名設定コマンドの詳細は３．６．１５章参照

→ マネージャ設定コマンドの詳細は３．６．１４章参照

→ 再起動コマンドの詳細は３．６．１３章参照

３．コマンドラインインターフェース

３．１　コマンドラインインターフェース概要

NQ では､コマンドラインインターフェースによって､NQ の設定を参照／変更することができます。コマンドラインインターフェースは、telnet を利用したネットワーク接続を介して NQ にアクセスすることで使用可能です。なお、NQ の設定を参照／変更する場合、認証コマンド（３．６．１章参照）を使用して各コマンドを実行可能な状態に遷移させる必要があります。
なお、本書の実行例は Windows PC のコマンドプロンプトを使用した場合として記載しています。その他のターミナルソフトを使用する場合は、実行例を参考に利用してください

３．２　telnetによるネットワーク接続

telnet を介した NQ へのネットワーク接続方法を以下に説明します。

[書式]

```
telnet <host>  23496
```

[説明]

NQ の 23496 番ポートへ telnet を介してネットワーク接続を行います。なお、使用ポートを変更することはできません。コマンドは、全て半角英数字で入力してください。
Tera Term を使用する場合、ツールバーから[File]→[New connection]を選択し、以下の設定を行ってください。

通信種別　：　TCP/IP
Host　　　　：　NQ の IP アドレス、またはホスト名
Service　　：　Telnet
TCP Port#：　23496

その他のターミナルソフトを使用する場合は、上記の内容を参考に接続先を指定してください。

[引数]

引数	説明
<host>	NQ の IP アドレスまたはホスト名

[実行例]

```
C:¥> telnet 192.168.250.250 23496
- 400 require authentication
svna>
```

[注意]

telnet を介した NQ へのネットワーク接続後、画面上にメッセージが出力されない、入力文字が表示されない、Enter キー入力による実行ができない場合の対処方法は、６．１章を参照してください。

３．３　認証前のネットワーク接続終了方法

［書式］

```
exit
```

［説明］

telnet を介して NQ へネットワーク接続した際に、認証コマンド（３．６．１章参照）実行前に接続を終了する場合は、以下のコマンドを実行してください。
なお、終了コマンド（３．６．１２章参照）とは異なり、quit コマンドは使用できません。

［実行例］

```
C:¥> telnet 192.168.250.250 23496      ネットワーク接続を行う
- 400 require authentication
svna> exit                             ネットワーク接続を終了する
+ Goodbye.

ホストとの接続が切断されました。
C:¥>
```

３．４　コマンド一覧

NQ でサポートするコマンドの一覧を以下に示します。本書で説明されていないコマンドはサポート対象外です。

説明	コマンド	参照
認証コマンド	pass	3.6.1 章
認証パスワード変更コマンド	set us	3.6.2 章
ネットワークインターフェース確認コマンド	list if	3.6.3 章
DNS サーバアドレス、ドメイン名確認コマンド	list ns	3.6.4 章
エージェント設定確認コマンド	list na	3.6.5 章
ネットワークインターフェース設定の反映タイミング変更コマンド	set if auto	3.6.6 章
ネットワークインターフェース設定コマンド	set if	3.6.7 章
エージェント設定コマンド	set na	3.6.8 章
DNS サーバアドレス設定コマンド	set ns nameserver	3.6.9 章
ドメイン名設定コマンド	set ns domain	3.6.10 章
ヘルプコマンド	help	3.6.11 章
終了コマンド	exit quit	3.6.12 章
再起動コマンド	reboot set na reboot	3.6.13 章
マネージャ設定コマンド	set sm	3.6.14 章
エージェント名設定コマンド	set hn	3.6.15 章
初期化コマンド	init all	3.6.16 章
シャットダウンコマンド	shutdown set na shutdown	3.6.17 章
ネットワークインターフェースのネゴシエーション設定確認コマンド	list ifspeed	3.6.18 章
ネットワークインターフェースのネゴシエーション設定変更コマンド	set ifspeed	3.6.19 章
VLAN インターフェース追加コマンド	add vlan eth0	3.6.20 章
VLAN インターフェース削除コマンド	remove vlan	3.6.21 章
デフォルトゲートウェイアドレス設定コマンド	set gw	3.6.22 章
DNS サーバアドレス削除コマンド	remove ns nameserver	3.6.23 章
エージェント開始コマンド	set na start	3.6.24 章
エージェント停止コマンド	set na stop	3.6.25 章
ドメイン名削除コマンド	remove ns domain	3.6.26 章
デフォルトゲートウェイアドレス削除コマンド	remove gw *	3.6.27 章
文字コード指定コマンド	charset	3.6.28 章
ネットワークリスト追加コマンド	add networklist	3.6.29 章
ネットワークリスト削除コマンド	remove networklist	3.6.30 章

３．５　コマンド入力時の注意・制限事項

- コマンド入力は、一部の引数の入力以外は半角文字を使用してください。エージェント設定コマンド（３．６．８章参照）を使用して、「AgentLocation」、「AdminName」、「AdminTelephoneNumber」の各項目（８．２章の該当項目を参照）を設定する場合のみ、引数に全角文字を入力することができます。
- 全角文字は、Shift_JIS、日本語 EUC（EUC-JP）の文字コードが利用できます。telnet クライアント PC の設定を確認の上、文字コード指定コマンド（３．６．２８章参照）を使用して NQ の文字コード設定を一致させてください。
- 入力文字が表示されない、Enter キー入力による実行ができない場合の対処方法は、６．１章を参照してください。
- 使用する telnet クライアント PC によっては、コマンド入力時に、[back space]、[delete]、方向キー等による入力文字の編集ができない場合があります。
- コマンド実行時に表示されるメッセージから、成功、およびエラーを確認してください。下記に主な表示メッセージを示します。

メッセージ	内容
Welcome to SvNaConsole.	認証成功
Goodbye.	telnet を介したネットワーク接続終了
Invalid command.	コマンド実行エラー（コマンド入力ミスなど）
Command succeeded.	コマンド実行成功
400 require authentication.	telnet を介したネットワーク接続成功
403 bad pass phrase.	認証エラー
404 maximum retries.	認証パスワード入力 3 回失敗時の接続切断通知
500 generic error.	一般エラー
501 system error.	システムエラー
502 no data.	データ（情報詳細）なし
503 invalid data.	不正なデータが設定
504 no record.	設定項目が見つからない

３．６　コマンドリファレンス

３．６．１　認証コマンド（pass）

［書式］

```
pass <password>
```

［説明］

認証コマンドを使用してログインすることで、NQ に対して全てのコマンドを実行可能な状態へ遷移します。telnet を介したネットワーク接続後は、本コマンドによって認証しなければ以降に説明するコマンドを利用できません。
<password> には認証パスワードを入力してください。
なお、認証パスワードはセキュリティ対策として既定値から変更することを推奨します。認証パスワードの変更方法は３．６．２章を参照してください。

［引数］

引数	説明
<password>	設定されている認証パスワード。 パスワードに使用可能な文字は、1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。8 バイト(文字)より長い場合は、以降の文字列は認識されません。引数は、４．２．１章の注意事項を参照の上、入力してください。工場出荷時の認証パスワードの既定値は『admin』です。

［実行例］

```
svna> pass admin
+ Welcome to SvNaConsole.
svna>
```

［注意］

設定とは異なる認証パスワードを入力してコマンドを実行した場合、認証エラーが合計 3 回に達した時点で NQ へのネットワーク接続が切断されます。認証パスワードを入力せず、pass コマンドのみでコマンドを実行した場合は、認証エラーのメッセージが表示されますが、認証エラーとしてカウントされません。

３．６．２　認証パスワード変更コマンド（set us）

［書式］

```
set us <user> <password>
```

［説明］

認証パスワードを変更します。

［引数］

引数	説明
<user>	ユーザ名。admin 固定です。
<password>	設定変更後に使用する認証パスワード。 パスワードに登録可能な文字は､1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。8 バイト(文字)より長い場合は、以降の文字列は認識されません。引数は、４．２．１章の注意事項を参照の上、入力してください。

［実行例］

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

認証パスワードを『abcxyz』に変更する

認証パスワードは、変更したパスワードが正しく設定されたことを確認する必要があります。以降の［確認手順］を参照し、確実に設定を行ってください。

[確認手順]

コマンド入力時に[back space]、[delete]、方向キー等による入力文字の編集ができない telnet クライアント PC を使用する場合、認証パスワード入力時に方向キーなどを押下すると、画面上に反映されなくても文字列として認識してしまうことがあります。
そのため、認証パスワードの変更時は、以下の手順で正常にログインできることを確認することを推奨します。手順は、コマンドプロンプトを使用した場合となります。

① 認証パスワードを変更する

telnet を介したネットワーク接続を行い、認証コマンドでログインした後、認証パスワード変更コマンドを使用して認証パスワードを変更してください。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

認証パスワードを変更する

② 新たにネットワーク接続を行う

①で接続中のコマンドプロンプトのネットワーク接続を終了させず、新たにコマンドプロンプトを起動させ、NQ へネットワーク接続を行ってください。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
C:¥> telnet 192.168.250.250 23496
- 400 require authentication
svna>
```

別のコマンドプロンプトから接続する

③ 新規接続から認証コマンドを実行する

②で NQ へ接続したコマンドプロンプトから認証コマンドを使用して、①で設定したパスワードでログイン可能か確認してください。パスワードが異なる場合は、認証エラーとなります。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
- 400 require authentication
svna> pass abc
- 403 bad pass phrase.
```

認証コマンドでログインできない場合

パスワードが正しい場合、正常にログインできます。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
svna> pass abcxyz
+ Welcome to SvNaConsole.
svna>
```

認証コマンドでログインできた場合

④ 新規接続から認証コマンドでログインできない場合

①で設定したパスワードを使用しても正常にログインできない場合、変更コマンド使用時に方向キー押下などによる不正な文字入力が含まれた可能性があります。①でログイン中のコマンドプロンプトより、認証パスワードを再設定し、③の確認手順を行ってください。

```
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

```
svna> pass abcxyz
- 403 bad pass phrase.
svna>
```

認証エラーとなった場合

↓

```
svna> set us admin abcxyz
+ Command succeeded.
svna> set us admin abcxyz
+ Command succeeded.
svna>
```

認証パスワードを再設定する

```
svna> pass abcxyz
- 403 bad pass phrase.
svna> pass abcxyz
+ Welcome to SvNaConsole.
svna>
```

認証コマンドでログインできる

３．６．３　ネットワークインターフェース確認コマンド（list if）

[書式]

```
list if
```

[説明]

ネットワークインターフェースの設定状態を表示します。

[実行例]

■非タグ VLAN 環境設置時の実行例

```
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.250.255
        Default Gateway:192.168.250.1
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna>
```

■タグ VLAN 環境設置時の実行例

```
svna> list if
= Command succeeded.
eth0    inet addr:127.0.0.1 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:127.0.0.255
        UP  BROCAST  RUNNING  MULTICAST
eth0.111        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.10.255
        Default Gateway:192.168.10.254
        UP  BROCAST  RUNNING  MULTICAST
eth0.112        inet addr:192.168.20.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.20.255
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna>
```

［表示項目］

項目	説明
eth0	ネットワークインターフェース
eth0.*	VLAN インターフェース（左記項目のアスタリスク（*）は VLAN ID）
inet addr	IP アドレス
HWaddr	MAC アドレス
Mask	サブネットマスク
Bcast	ブロードキャストアドレス
Default Gateway	デフォルトゲートウェイアドレス

３．６．４　DNSサーバアドレス、ドメイン名確認コマンド（list ns）

[書式]

```
list ns
```

[説明]

DNS サーバの IP アドレス、ドメイン名を表示します。

[実行例]

```
svna> list ns
= Command succeeded.
nameserver 192.168.0.6
nameserver 192.168.0.7
domain isnq.dom
+ Done.
svna>
```

[表示項目]

項目	説明
nameserver	DNS サーバの IP アドレス
domain	NQ が属するドメイン名

３．６．５　エージェント設定確認コマンド（list na）

［書式］

```
list na
```

［説明］

エージェント設定を表示します。確認可能な項目については、８章を参照してください。

［表示形式］

本コマンドを実行した場合、属性名と属性値が同一行に表示されます。

属性名は、アルファベット順にソートされた状態で表示されます。

属性名と属性値は、以下の形式で表示されます。

```
属性名: 属性値
```

［実行例］

```
svna> list na
= Command succeeded.
AdminMailAddress: admin@securevisor.dom
…
+ Done.
svna>
```

３．６．６　ネットワークインターフェース設定の反映タイミング変更コマンド（set if auto）

[書式]

```
set if auto { on | off }
```

[説明]

ネットワークインターフェース設定コマンド（３．６．７章参照）を実行した時に、設定内容が反映されるタイミングを変更します。設定が有効（*on*）の場合、ネットワークインターフェース設定コマンドによる設定内容は、コマンド実行直後に反映されます。設定が無効（*off*）の場合は、NQ の再起動時に反映されます。初期状態では無効が設定されています。

本設定が有効の場合、ネットワークインターフェース設定コマンドを使用して IP アドレスなどを変更すると、コマンド実行直後に反映され、NQ へのネットワーク接続が切断されることがありますので注意してください。

[実行例]

```
svna> set if auto off
+ Command succeeded.
svna>
```

３．６．７　ネットワークインターフェース設定コマンド（set if）

［書式］

```
set if 〈nic〉 [address 〈address〉] [mask 〈mask〉]
```

［説明］

ネットワークインターフェース設定を行います。set if、または set if 〈*nic*〉のみを実行した場合は、エラーとなります。

［引数］

引数	説明
〈*nic*〉	設定対象のインターフェース。 非タグ VLAN 環境設置時は『eth0』を指定してください。 VLAN インターフェース設定時は『eth0.〈*vid*〉(※)』を指定してください。
〈*address*〉	インターフェースに設定する IP アドレス。引数は、４．１章の注意事項を参照の上、入力してください。設定可能な範囲は、『1.0.0.1』～『223.255.255.254』までとなります。 NQ をタグ VLAN 環境に設置する場合、ネットワークインターフェースである『eth0』と VLAN インターフェースである『eth0.〈*vid*〉(※)』に設定する IP アドレスの重複を避けるため、『eth0』に『127.0.0.1』を設定してください。
〈*mask*〉	インターフェースに設定するサブネットマスク。引数は、４．１章の注意事項を参照の上、入力してください。設定可能な範囲は、『255.0.0.0』の 8 ビットから『255.255.255.252』の 30 ビットまでとなります。 NQ をタグ VLAN 環境に設置する場合、ネットワークインターフェースである『eth0』に対してサブネットマスクを設定する必要はありません。

（※）〈*vid*〉は VLAN 設定インターフェース追加コマンド（３．６．２０章参照）で指定した VLAN ID

[実行例]

■非タグ VLAN 環境設置時

```
svna> set if auto off
+ Command succeeded.
svna> set if eth0 address 192.168.250.250 mask 255.255.255.0
+ Command succeeded.
svna> reboot
+ Command succeeded.
```

→ネットワークインターフェース設定の反映タイミング変更コマンドの詳細は３．６．６章参照

→ネットワークインターフェース設定コマンドの詳細は本章参照

→ネットワークインターフェース設定の反映タイミング変更コマンドを無効に設定した場合は再起動コマンド（３．６．１３章参照）が必須となります

■タグ VLAN 環境設置時

```
svna> set if auto off
+ Command succeeded.
svna> add vlan eth0 111
+ Command succeeded.
svna> set if eth0 address 127.0.0.1
+ Command succeeded.
svna> set if eth0.111 address 211.10.10.200 mask 255.255.255.0
+ Command succeeded.
svna> reboot
+ Command succeeded.
```

→ネットワークインターフェース設定の反映タイミング変更コマンドの詳細は３．６．６章参照

→VLAN インターフェース追加コマンドの詳細は３．６．２０章参照

→ネットワークインターフェース設定コマンドの詳細は本章参照

→VLAN インターフェースの設定を反映させるには、再起動コマンド（３．６．１３章参照）が必須となります

[注意]

NQ をタグ VLAN 環境に設置する場合、VLAN インターフェース追加コマンド（３．６．２０章参照）を実行後、VLAN インターフェースに指定した VLAN ID を使用して本コマンドを実行してください。また、ネットワークインターフェースと VLAN インターフェースの IP アドレスの重複を避けるため、『eth0』の address の設定値に『127.0.0.1』を設定してください。VLAN インターフェースの設定を行った場合、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（３．６．１３章）を実行してください。

非タグ VLAN 環境設置時に、本コマンドで IP アドレス変更後、NQ の再起動を実施した場合、エージェント設定（４章参照）の IpAddress、CollectIpAddress、NetworkAddress、NetworkMask の各属性値は、自動的に本コマンドの設定値が反映されます。

なお、ネットワークインターフェース設定の反映タイミング変更コマンド（３．６．６章参照）を無効に設定していない場合、本コマンド実行直後に IP アドレスなどの変更が反映され、NQ へのネットワーク接続が切断されることがあります。本コマンド実行時は、ネットワークインターフェース設定の反映タイミング変更コマンドは無効に設定し、全ての設定を変更後、NQ を再起動させる手順を強く推奨します。

３．６．８　エージェント設定コマンド（set na）

[書式]

```
set na <attribute> <value>
```

[説明]

エージェントの属性を設定します。設定可能な属性は８．２章を参照してください。

[引数]

引数	説明
<attribute>	属性名
<value>	属性値

[実行例]

```
svna> set na stop                               →エージェント停止コマンドの詳細は
+ Command succeeded.                              ３．６．２５章参照
svna> set na ManagerIpAddress 192.168.250.251
+ Command succeeded.
svna> set na start                              →エージェント開始コマンドの詳細は
+ Command succeeded.                              ３．６．２４章参照
```

[注意]

本コマンドを使用する前に、エージェント停止コマンド（３．６．２５章参照）を使用してNetworkAgent サービスを停止してください。

本コマンドを使用してエージェント属性を変更した場合、設定内容を反映させるため、エージェント開始コマンド（３．６．２４章参照)、あるいは再起動コマンド（３．６．１３章参照）を実行してください。(※)

（※）　VLAN インターフェースの追加など、設定内容の反映に NQ の再起動が必要となる操作を併せて実施している場合は、必ず再起動を行ってください。

３．６．９　DNSサーバアドレス設定コマンド（set ns nameserver）

[書式]

```
set ns nameserver <server1> [<server2>...]
```

[説明]

DNS サーバの設定を行います。DNS サーバの設定を行った場合、収集したホストの IP アドレスから DNS 名の逆引きが可能となり､取得した DNS 名を SiteManager へ通知することができます。

[引数]

引数	説明
<server1>...	DNS サーバの IP アドレス。最大 3 個まで設定可能。引数は、４．１章の注意事項を参照の上、入力してください。複数の DNS サーバアドレスを設定する場合は、引数の間に半角スペースを入れてください。

[実行例]

```
svna> set ns nameserver 192.168.250.6 192.168.250.7
+ Command succeeded.
svna>
```

３．６．１０　ドメイン名設定コマンド（set ns domain）

［書式］

```
set ns domain <domain1> [<domain2>...]
```

［説明］

ドメイン名の設定を行います。

［引数］

引数	説明
<domain1>...	DNS のドメイン名。複数のドメイン名を設定する場合は、引数の間に半角スペースを入れてください。

［実行例］

```
svna> set ns domain isnq.dom
+ Command succeeded.
svna>
```

［注意］

本コマンドは、パラメータに設定可能な文字数は 2,000 文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれますので注意してください。

３．６．１１　ヘルプコマンド（help）

［書式］

```
help [<command>]
```

［説明］

コマンドのヘルプ情報を表示します。help のみを実行した場合はコマンド一覧を表示します。help で表示されるコマンドであっても、本書で説明されていないコマンドの使用はサポート対象外となりますので注意してください。

［引数］

引数	説明
<command>	使用方法を確認したいコマンド名

［実行例］

```
svna> help set
= Usage of set command:
set if <nic> [address <address>] [mask <mask>]
set if <nic> [on|off]
set na <attribute> <value>
set na [start|stop|restart|reboot|shutdown]
set ns nameserver <server1> [<server2>...]
set ns domain <domain1> [<domain2>...]
set ns local <hostname>
set us <user> <password>
set ifspeed [100fd|100hd|10fd|10hd|auto]
set gw <defaultgateway>
+ Done.
svna>
```

３．６．１２　終了コマンド（exit, quit）

［書式］

```
exit
または
quit
```

［説明］

telnetを介したネットワーク接続を終了します。認証コマンド（３．６．１章参照）による認証後は、exitコマンドとquitコマンドに動作の差異はありません。

［実行例］

```
svna> exit
+ Goodbye.



ホストとの接続が切断されました。
```

３．６．１３　再起動コマンド（reboot，set na reboot）

［書式］

```
reboot
または
set na reboot
```

［説明］

NQ を再起動します。reboot コマンドと set na reboot コマンドに動作の差異はありません。

［実行例］

```
svna> reboot
```

３．６．１４　マネージャ設定コマンド（set sm）

[書式]

```
set sm <address>
```

[説明]

SiteManager をインストールしている PC の IP アドレスを設定します。

[引数]

引数	説明
<address>	NQ の管理／操作を行う SiteManager インストール PC の IP アドレスを設定します。引数は、４．１章の注意事項を参照の上、入力してください。ホスト名で設定することはできません。

[実行例]

```
svna> set na stop                     →エージェント停止コマンドの詳細は
+ Command succeeded.                    ３．６．２５章参照
svna> set sm 192.168.250.251
+ Command succeeded.
svna> set na start                    →エージェント開始コマンドの詳細は
+ Command succeeded.                    ３．６．２４章参照
```

[注意]

本コマンドを使用する前に、エージェント停止コマンド（３．６．２５章参照）を使用して NetworkAgent サービスを停止してください。

本コマンドを使用して SiteManager インストール PC の IP アドレスを変更した場合、設定内容を反映させるため、エージェント開始コマンド（３．６．２４章参照）、あるいは再起動コマンド（３．６．１３章参照）を実行してください。(※)

（※）　VLAN インターフェースの追加など、設定内容の反映に NQ の再起動が必要となる操作を併せて実施している場合は、必ず再起動を行ってください。

３．６．１５　エージェント名設定コマンド（set hn）

［書式］

```
set hn 〈agentname〉
```

［説明］

エージェント名を設定します。

［引数］

引数	説明
〈agentname〉	サイトコンソールに表示するエージェント名を設定します。 引数は、４．３章の注意事項を参照の上、入力してください。

［実行例］

```
svna> set na stop
+ Command succeeded.
svna> set hn isnq30
+ Command succeeded.
+ Command succeeded.
svna> reboot
+ Command succeeded.
```

→エージェント停止コマンドの詳細は３．６．２５章参照

→ 再起動コマンドの詳細は３．６．１３章参照

［注意］

*〈agentname〉*へ登録可能な文字は、半角英数字、ハイフン(-)、アンダーバー(_)、ドット(.)、小括弧((,))からなる1バイト(文字)以上32バイト(文字)以下の文字列で、大文字、小文字は区別されません。また、以下に該当する文字列を設定した場合は、SiteManagerに登録することができません。

●Windows予約デバイス名(AUX、CON、NUL、PRN、COM0～COM9、LPT0～LPT9)
●エージェント名の先頭、あるいは末尾がドット(.)である

『isnq30(1)』のように文字列の末尾に小括弧で囲んだ半角数字を記述する場合、SiteManagerオンラインヘルプを参照し、サイトコンソールのエージェント設定ダイアログから行ってください。
本コマンドを使用する前に、エージェント停止コマンド（３．６．２５章参照）を使用してNetworkAgentサービスを停止してください。
また、本コマンドを使用してエージェント名を設定した場合は、NQの再起動が必要となります。全ての設定を登録後、再起動コマンド（３．６．１３章参照）を実行してください。

３．６．１６　初期化コマンド（init all）

［書式］

```
init all
```

［説明］

エージェントのネットワーク設定を工場出荷時の値（既定値）に戻します。ただし、現在は制限事項（５章参照）があります。工場出荷時の値については８章を参照してください。

初期化される項目は以下の通りです。

初期化内容	パラメータ	初期値
IP アドレス	IpAddress	192.168.250.250
NQ が SiteManager との通信に使用する IP アドレス	CollectIpAddress	192.168.250.250
NQ が SiteManager からの通信を受信するポート番号	Port	23491
マネージャへの通信に使用する宛先ポート番号	ManagerPort	23490
ネットワークマスク	NetworkMask	255.255.255.0
ネットワークアドレス	NetworkAddress	192.168.250.0
デフォルトゲートウェイアドレス	DefaultGateway	192.168.250.1
マネージャアドレス	ManagerIpAddress	192.168.250.251
エージェント名・ホスト名	AgentName	isnq30
不正接続防止設定状態	JamStatus	Off
データ収集設定状態	CollectOfPacket	Off
NQ が SiteManager にホスト情報を通知するインターバル	NotifyInterval	60

［実行例］

```
svna> set na stop
+ Command succeeded.
svna> init all
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
+ Command succeeded.
svna> reboot
+ Command succeeded.
```

→エージェント停止コマンドの詳細は
３．６．２５章参照

→再起動コマンドの詳細は
３．６．１３章参照

［注意］

本コマンドを使用する前に、エージェント停止コマンド（３．６．２５章参照）を使用して NetworkAgent サービスを停止してください。

本コマンドを使用して工場出荷時に戻した場合は、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（３．６．１３章参照）を実行してください。

３．６．１７　シャットダウンコマンド（shutdown、set na shutdown）

[書式]

```
shutdown
または
set na shutdown
```

[説明]

NQ を停止させます。shutdown コマンドと set na shutdown コマンドに動作の差異はありません。NQ 停止後、再度起動させる場合は電源ケーブルの抜き差しを行ってください。NQ30a、NQ30c の場合は、電源スイッチ押下でも起動可能です。

[実行例]

```
svna> shutdown
```

３．６．１８　ネットワークインターフェースのネゴシエーション設定確認コマンド(list ifspeed)

[書式]

```
list ifspeed
```

[説明]

NQ のネットワークインターフェースのネゴシエーション設定を表示します。

[実行例]

```
svna> list ifspeed
eth0: no autonegotiation, 10baseT-HD, link ok
+ Command Succeeded.
svna>
```

３．６．１９　ネットワークインターフェースのネゴシエーション設定変更コマンド（set ifspeed）

[書式]

```
set ifspeed { auto | 100FD | 100HD | 10FD | 10HD }
```

[説明]

NQ のネットワークインターフェースのネゴシエーション設定を変更します。

[引数]

引数	説明
auto	オートネゴシエーションを設定します。工場出荷時は、既定値としてオートネゴシエーションが設定されています。 本引数が指定された場合、オートネゴシエーションのリスタートが実行されます。
100FD	100baseTx 全二重通信を設定します。
100HD	100baseTx 半二重通信を設定します。
10FD	10baseT 全二重通信を設定します。
10HD	10baseT 半二重通信を設定します。

[実行例]

```
svna> set ifspeed auto
resetting the transceiver...
+ Command Succeeded.
svna>
```

[注意]

ネットワークインターフェースのネゴシエーション設定を変更する場合、接続先ポートと異なる設定を実施すると、正常に接続できなくなる可能性があります。変更時は、接続先の設定を確認して実施してください。

なお、NQ のネットワークインターフェースのネゴシエーション設定は、NQ の再起動後も設定内容が継続されます。

３．６．２０　VLANインターフェース追加コマンド（add vlan eth0）

［書式］

```
add vlan eth0 <vid>
```

［説明］

NQ の VLAN インターフェースを追加します。NQ に VLAN ID を割り当てた VLAN インターフェースを作成することで、該当の VLAN ID のタグ付きパケットを収集することができます。VLAN ID には、実際にネットワークで使用している VLAN ID を設定してください。

［引数］

引数	説明
<vid>	VLAN ID を設定します。VLAN インターフェースは、設定された VLAN ID によって作成されます。 VLAN ID は、10 進数で『0』～『4094』の値が設定可能です。

［実行例］

```
svna> add vlan eth0 111
+ Command Succeeded.
svna> set if eth0.111 address 211.10.10.200 mask 255.255.255.0
+ Command Succeeded.        →ネットワークインターフェース設定コマンドの詳細は
                              ３．６．７章参照
svna>
svna> add vlan eth0 111     →登録済みの VLAN ID を追加した場合はエラーとなります
 vlan interface already exist
+ Command failed.
svna> reboot                →VLAN インターフェースの設定を反映させるには、
+ Command succeeded.          再起動コマンド（３．６．１３章参照）が必須となります
```

［注意］

追加する VLAN ID が既に NQ に登録済みの場合、エラーメッセージが表示され、登録することができません。

なお、本コマンドを実行後、設定を反映させるには、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（３．６．１３章参照）を実行してください。

再起動後、ネットワークインターフェース確認コマンド（３．６．３章参照）で設定を確認してください。

３．６．２１　VLANインターフェース削除コマンド（remove vlan）

［書式］

```
remove vlan <nic>
```

［説明］

NQ の VLAN インターフェースを削除します。VLAN インターフェース単位、または一括での削除が指定可能です。

［引数］

引数	説明
<nic>	NQ の VLAN インターフェース単位で削除する場合は eth0.*<vid>*（※）を設定してください。 全ての VLAN インターフェースを削除する場合、アスタリスク（*）を設定してください。 （※）*<vid>* は VLAN インターフェース追加コマンド（３．６．２０章参照）で指定した VLAN ID

［実行例］

```
svna> list if                         →ネットワークインターフェース確認コマンドの詳細は
= Command succeeded.                    ３．６．３章参照
eth0    inet addr:127.0.0.1 HWaddr 00:00:4c:11:22:33
        Mask:255.0.0.0  Bcast:127.255.255.255
        UP  BROCAST  RUNNING  MULTICAST
eth0.111        inet addr:192.168.10.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.10.255
        Default Gateway:192.168.10.254     →不要な VLAN インターフェースが設定
        UP  BROCAST  RUNNING  MULTICAST      されている場合、削除してください
+ Done.
svna> remove vlan eth0.111
+ Command Succeeded.
svna> reboot                          →VLAN インターフェースの設定を反映させるには、
+ Command succeeded.                    再起動コマンド（３．６．１３章参照）が必須となります
```

［注意］

本コマンドを実行後、設定を反映させるには、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（３．６．１３章参照）を実行してください。

再起動後、ネットワークインターフェース確認コマンド（３．６．３章参照）で設定を確認してください。

３．６．２２　デフォルトゲートウェイアドレス設定コマンド（set gw）

[書式]

```
set gw <gateway>
```

[説明]

デフォルトゲートウェイアドレスを設定します。

[引数]

引数	説明
<gateway>	デフォルトゲートウェイアドレスを設定。 ４．１章を参照して、デフォルトゲートウェイアドレスを入力してください。

[実行例]

```
svna> set gw 10.1.2.254
+ Command Succeeded.
svna> reboot
+ Command succeeded.
```

→デフォルトゲートウェイアドレスの設定を反映させるには、再起動コマンド（３．６．１３章参照）が必須となります

[注意]

本コマンドを実行後、設定を反映させるには、NQ の再起動が必要となります。全ての設定を登録後、再起動コマンド（３．６．１３章参照）を実行してください。

３．６．２３　DNSサーバアドレス削除コマンド（remove ns nameserver）

[書式]

```
remove ns nameserver <server1> [<server2>...]
```

[説明]

DNS サーバの設定を削除します。DNS サーバの IP アドレス単位、または一括での削除が指定可能です。

[引数]

引数	説明
<server1>...	DNS サーバの IP アドレスを指定して削除する場合は、４．１章の注意事項を参照の上、入力してください。最大 3 個まで設定可能です。複数の DNS サーバアドレスを入力する場合は、引数の間に半角スペースを入れてください。 一括で削除する場合はアスタリスク（*）を入力してください。なお、引数に IP アドレスとアスタリスクを併用して入力した場合、削除処理が行われません。

[実行例]

```
svna> list ns
= Command succeeded.
nameserver 192.168.0.6
nameserver 192.168.0.7
domain isnq.dom
+ Done.
svna> remove ns nameserver 192.168.0.6 192.168.0.7
+ Command succeeded.
svna> list ns
= Command succeeded.
domain isnq.dom
+ Done.
svna>
```

→DNS サーバ、ドメイン名確認コマンドの詳細は３．６．４章参照

→DNS サーバアドレス削除コマンドによって設定値が削除される

３．６．２４　エージェント開始コマンド（set na start）

［書式］

```
set na start
```

［説明］

NetworkAgent サービスを開始します。

［実行例］

```
svna> set na start
+ Command succeeded.
svna> set na start
- 501 サービスはすでに開始しています。
svna>
```

→NetworkAgent サービスを多重起動させることはできません。

［注意］

NetworkAgent サービスは、NQ 起動時に開始されます。本コマンドは、エージェント停止コマンド（３．６．２５章参照）を使用して NetworkAgent サービスを停止した時に使用してください。

３．６．２５　エージェント停止コマンド（set na stop）

［書式］

```
set na stop
```

［説明］

NetworkAgent サービスを停止します。

［実行例］

```
svna> set na stop
+ Command succeeded.
svna> set na stop
- 501 サービスはすでに停止しています。  →NetworkAgent サービスが停止していれば
                                           エラーとなります。
svna>
```

［注意］

NetworkAgent サービスは、NQ 起動から 1 分以内、あるいはエージェント開始コマンド（３．６．２４章参照）実行から 30 秒以内は正常に停止できない場合があります。

本コマンドは、前述の時間を目安として一定時間経過後、使用してください。

３．６．２６　ドメイン名削除コマンド（remove ns domain）

［書式］

```
remove ns domain <domain1> [<domain2>...]
```

［説明］

ドメイン名の設定を削除します。ドメイン名単位、または一括での削除が指定可能です。

［引数］

引数	説明
<domain1>...	ドメイン名単位で削除する場合は、ドメイン名を指定してください。複数のドメイン名を入力する場合は、引数の間に半角スペースを入れてください。設定可能な文字数の合計は 2,000 文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれます。 一括で削除する場合はアスタリスク（*）を設定してください。なお、引数にドメイン名とアスタリスクを併用して入力した場合、削除処理が行われません。

［実行例］

```
svna> list ns
= Command succeeded.
nameserver 192.168.0.6
domain isnq.dom
+ Done.
svna> remove ns domain isnq.dom
+ Command succeeded.
svna> list ns
= Command succeeded.
nameserver 192.168.0.6
+ Done.
svna>
```

→DNS サーバ、ドメイン名確認コマンドの詳細は
３．６．４章参照

→ドメイン名削除コマンドによって設定値が
削除される

３．６．２７　デフォルトゲートウェイアドレス削除コマンド（remove gw）

[書式]

```
remove gw *
```

[説明]

デフォルトゲートウェイアドレスの設定を削除します。

[実行例]

```
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.250.255
        Default Gateway:192.168.250.1
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> remove gw *
+ Command Succeeded.
svna> reboot
+ Command succeeded.
```

→ネットワークインターフェース確認コマンドの詳細は３．６．３章参照

→デフォルトゲートウェイアドレスの削除を反映させるには、再起動コマンド（３．６．１３章参照）が必須となります

３．６．２８　文字コード指定コマンド（charset）

［書式］

```
charset { sjis | eucjp }
```

［説明］

NQ の文字コード指定を設定します。「AgentLocation」、「AdminName」、「AdminTelephoneNumber」の各項目（８．２章の該当項目を参照）で全角文字を入力する前に、telnet クライアント PC が使用する文字コードに合わせて変更してください。本コマンドを実行しない場合、文字コードは Shift_JIS として処理されます。

［引数］

引数	説明
sjis	Shift_JIS を設定します。
eucjp	日本語 EUC（EUC-JP）を設定します。

［実行例］

```
svna> charset eucjp
+ Command succeeded.
svna> set na stop                    →エージェント停止コマンドの詳細は３．６．２５章参照
+ Command succeeded.
svna> set na AgentLocation ” ○×ビル 4F”
+ Command succeeded.                 →エージェント設定コマンドの詳細は３．６．８章参照
                                       「AgentLocation」の詳細は、８．２章参照
svna> set na start
+ Command Succeeded.                 →エージェント開始コマンドの詳細は３．６．２４章参照
```

［注意］

NQ に指定された文字コードと、telnet クライアント PC が使用する文字コードが異なる場合、全角文字を反映させることができません。telnet クライアント PC の設定を確認の上、NQ の文字コード設定を一致させてください。なお、Windows のコマンドプロンプトの場合、既定値で Shift_JIS が設定されています。

３．６．２９　ネットワークリスト追加コマンド（add networklist）

［書式］

```
add networklist <address>/<mask>
```

［説明］

監視対象ネットワークリストにネットワークを追加します。共有ネットワーク対応機能の個別指定モード(※)を使用する場合、本コマンドで監視するネットワークを追加します。
現在設定されているネットワークリストを参照する場合、３．６．５章の list na コマンドを実行し、NetworkList の項目を参照してください。

(※)エージェントの所属する VLAN に設定されたサブネットのうち、本コマンドでネットワークリストに追加されたサブネットについて、収集した情報の全てをホスト一覧に表示します。ネットワークリストに追加されていないサブネットについては、MAC アドレスのみをホスト一覧に表示します。詳細は、SiteManager オンラインヘルプの[その他の機能]－[共有ネットワーク対応機能]を参照してください。

［引数］

引数	説明
Address	監視対象とするネットワークのアドレス。
Mask	監視対象ネットワークのサブネットマスク。8～30 まで指定可能です。

［実行例］

```
svna> add networklist 192.168.10.0/24
+ Command succeeded.
```

３．６．３０　ネットワークリスト削除コマンド（remove networklist）

[書式]

remove networklist <*address*>/<*mask*>

[説明]

ネットワークリスト追加コマンドで追加したネットワークを、監視対象ネットワークリストから削除します。すべてのネットワークを削除する場合は「<*address*>/<*mask*>」の代わりにアスタリスク（*）を指定します。
現在設定されているネットワークリストを参照する場合、３．６．５章の list na コマンドを実行し、NetworkList の項目を参照してください。

[引数]

引数	説明
address	ネットワークリストから削除するネットワークのアドレス。
mask	監視対象ネットワークのサブネットマスク。8～30 まで指定可能です。

[実行例]

```
svna> remove networklist 192.168.10.0/24
+ Command succeeded.
svna> remove networklist *
+ Command succeeded.
```

→特定のネットワークを監視対象ネットワークリストから削除

→すべての監視対象ネットワークを削除

４．設定値の記述、入力に関する注意事項

４．１　IPアドレス、サブネットマスク、デフォルトゲートウェイアドレス記述時の注意事項

SecureVisor では、各設定に使用する IP アドレス、サブネットマスク、デフォルトゲートウェイアドレスは、IPv4 のみサポートしています。設定値は、10 進数で記述した 4 つのオクテットをドット（.）で繋いだ形式で記述してください。各オクテットとドットの間にスペースを記述する、またはオクテットの先頭桁に 0 を記述する場合、設定が正常に反映されません。

192.168.10.250　→ 正常に反映されます
192.168.△10.250 → 第 3 オクテットにスペース(△)があるため、不正となります
192.168.010.250 → 第 3 オクテットの先頭桁に『0』があるため、不正となります

４．２　文字列記述時の注意事項

４．２．１　認証パスワードに関する注意事項

対象パラメータ		注意事項
設定方法	パラメータ	
設定ファイル	Password →７．１章参照	設定値に半角スペースが存在する場合、『"aaa bbb"』のように設定値をダブルクォート（"）、あるいはシングルクォート（'）で囲んでください。 ダブルクォート、またはシングルクォートで設定値を囲んでいる際に、設定値にダブルクォート、シングルクォート、円マーク（¥）の半角記号文字が含まれている場合、『"aaa ¥"bbb"』のように該当文字の前にEscape文字として円マークを記述してください。 文字列を囲むためのダブルクォート、シングルクォート、およびEscape文字は、文字数制限に含まれません。
ネットワーク接続	認証コマンド →３．６．１章参照 認証パスワード変更コマンド →３．６．２章参照	

［注意］
通常は、半角スペースを認証パスワードの文字列として認識しません。文字列中に半角スペースがある場合、半角スペースより前の文字列のみ認識します。

■設定ファイルの場合

```
Password:pass wd
```

■コマンド入力の場合

```
svna> pass pass wd
または
svna> set us admin pass wd
```

→ 上記の場合、『pass wd』は『pass』として認識します。

認証パスワードに半角スペースを含める場合、ダブルクォート（"）、またはシングルクォート（'）で文字列を囲んでください。文字列を囲むためのダブルクォート、シングルクォートは、文字数制限に含まれません。

■設定ファイルの場合

```
Password:”pass wd”
```

■コマンド入力の場合

```
svna> pass ”pass wd”
または
svna> set us admin ’pass wd’
```

→ 上記の場合、『”pass wd”』、または『’pass wd’』は『pass wd』として認識します。

文字列の先頭にダブルクォート、またはシングルクォートがある場合、次にダブルクォート、シングルクォートが現れる位置までを認証パスワードと見なします。

■設定ファイルの場合

```
Password:”pass”wd”
```

■コマンド入力の場合

```
svna> pass ”pass”wd”
または
svna> set us admin ’pass’wd’
```

→ 上記の場合、『”pass”wd”』、または『’pass’wd’』は『pass』として認識します。

ダブルクォート、またはシングルクォートで文字列を囲む際に、文字列中に円マーク（¥）、ダブルクォート、シングルクォートを使用する場合は、該当文字の前に Escape 文字として円マークを設定することで認証パスワードと見なします。文字列を囲むためのダブルクォート、および Escape 文字は、文字数制限に含まれません。

■設定ファイルの場合

```
Password:”pass¥”wd”
```

■コマンド入力の場合

```
svna> pass ”pass¥”wd”
または
svna> set us admin ’pass¥”wd’
```

→ 上記の場合、『”pass¥”wd”』、または『’pass¥”wd’』は『pass”wd』として認識します。

ダブルクォート、またはシングルクォートで文字列を囲んだ場合も、1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、および半角記号のみ登録できます。8 バイト(文字)より長い場合、以降の文字列は認識されません。

■設定ファイルの場合

```
Password:"passwd12345"
```

■コマンド入力の場合

```
svna> pass "passwd12345"
または
svna> set us admin 'passwd12345'
```

→ 上記の場合、『"passwd12345"』、または『'passwd12345'』は『passwd12』として認識します。

ダブルクォート、シングルクォートが文字列の先頭に設定されているが、以降の文字列にダブルクォート、シングルクォートが含まれていない場合、あるいは文字列の先頭以降にダブルクォート、シングルクォートが設定されている場合は、ダブルクォート、シングルクォートを認証パスワードの文字列の一部として設定します。

■設定ファイルの場合

```
Password:"passwd
```

■コマンド入力の場合

```
svna> pass pass"wd"
または
svna> set us admin pass'wd'
```

→ 上記の場合、『"passwd』は『"passwd』、『pass"wd"』は『pass"wd"』、『pass'wd'』は『pass'wd'』として認識します。

４．２．２　認証パスワード以外の文字列に関する注意事項

対象パラメータ		注意事項
設定方法	パラメータ	
設定ファイル	AgentLocation AdminName AdminTelephoneNumber →７．４章参照	文字列中に円マーク（¥)、ダブルクォート（″)、シングルクォート（'）の半角記号文字が存在する場合、『aaa ¥″bb』のように該当文字の前にEscape 文字として円マークを記述してください。Escape 文字は、文字数制限に含まれません。 なお、設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。
ネットワーク接続	AgentLocation AdminName AdminTelephoneNumber →８．２章参照	文字列中に半角スペースが存在する場合、ダブルクォート（″)、またはシングルクォート（'）で文字列を囲んでください。ダブルクォート、またはシングルクォートで文字列を囲んでいる際に、文字列中に円マーク（¥)、ダブルクォート（″)、シングルクォート（'）の半角記号文字が存在する場合、『″aaa ¥″bb″』のように該当文字の前にEscape 文字として円マークを記述してください。Escape 文字は、文字数制限に含まれません。 なお、設定値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。

４．３　エージェント名記述時の注意事項

AgentName（エージェント名）は、このエージェントが登録されている SiteManager が管理する他のエージェントと重複しないように設定してください。SiteManager に既に同名のエージェントが登録されている場合は、「AgentName(1)」のような括弧数字付きの名前となりますので、別の名前に変更してください。

５．制限事項

・ NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合は、電源スイッチを押下してください。機器を停止させる場合は、以下のいずれかを実行してください。

●シャットダウンコマンド（３．６．１７章参照）を実行する（推奨）

●電源スイッチを 5 秒以上押し続ける

●電源ケーブルを抜く

・ NQ30b は、電源スイッチがありません。電源ケーブルの接続により、自動起動します。機器を停止させる場合は、以下のいずれかを実行してください。

●シャットダウンコマンド（３．６．１７章参照）を実行する（推奨）

●電源ケーブルを抜く

・ 初期化コマンド（３．６．１６章参照）では一部のネットワーク設定が工場出荷状態に戻りません。全てのネットワーク設定を変更する場合、下記の項目を参照し、設定値の変更、または１．８章を参照して初期化を行ってください。

項目	使用コマンド	参照	初期設定値
認証パスワード	set us	３．６．２章	admin
DNS サーバアドレス	remove ns nameserver	３．６．２３章	なし
ドメイン名	set ns domain	３．６．１０章	isnq.dom
VLAN インターフェース	remove vlan	３．６．２１章	なし

・ NQ では、NetBEUI プロトコルのパケットを解析できません。そのため、SiteManager のホスト一覧上で、NetBEUI フラグのチェックがつきません。また、NetBEUI しか利用しない端末の検知、防止ができません。

・ USB メモリを使用したセットアップ方法によってタグ VLAN 環境から非タグ VLAN 環境での使用に切り替える場合、NQ の電源再起動などで設定ファイルを認識させる前に、ネットワークインターフェース設定コマンド（３．６．７章参照）を使用し、『eth0』の IP アドレスを設定する必要があります。前述の手順を行わずに設定ファイルを認識させた場合、NQ 起動後にもう一度 NQ の再起動が必要となることがあります。

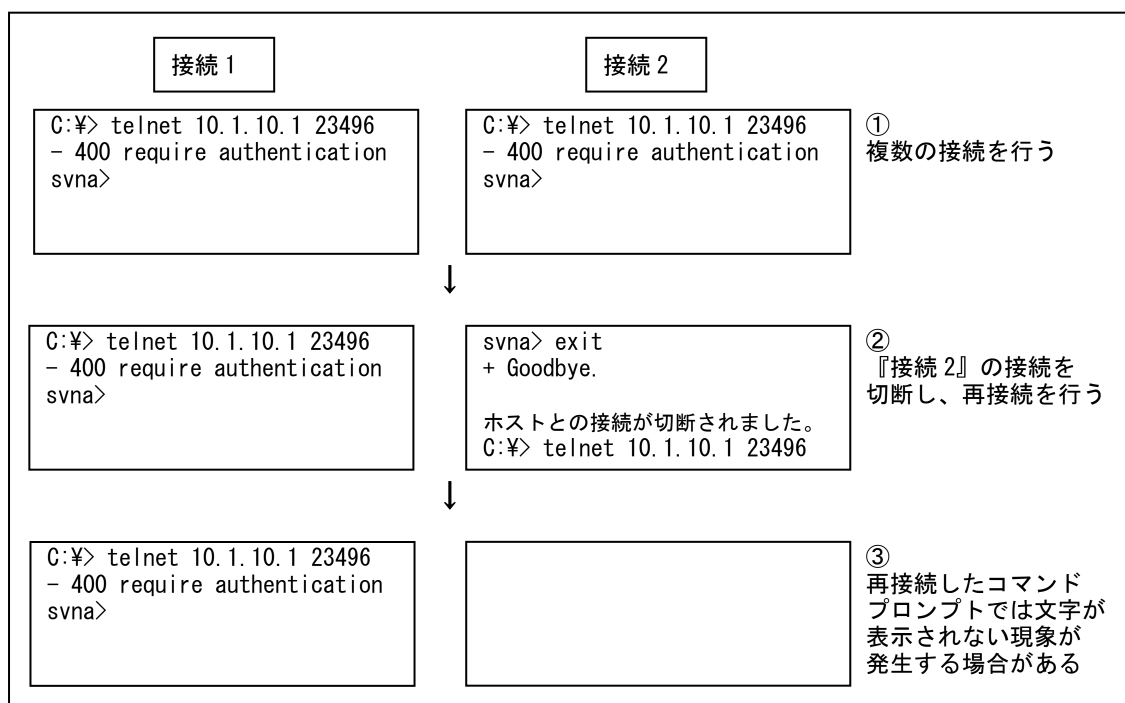
・ Ver3.3 未満のバージョンからバージョンアップした場合、list if コマンドで表示される、Bcast の値が、Mask から求められる値と異なる値で表示されます。NQ はこの値を用いて通信することはありませんので、そのままご利用していただいて問題ありません。また、ネットワークマスクを再度設定すれば、不正な表示は解消されます。

６．トラブルシューティング

６．１　NQへのネットワーク接続時に文字が正常に表示されない

telnet を介して NQ に接続した時に、出力文字が正常に表示されない、入力文字が表示できない場合、以下を確認してください。

■同一の NQ に対して複数のネットワーク接続を行っている場合
同一の NQ に対して複数のネットワーク接続を行っている時に、一部の接続を切断すると、切断処理が正常に終了できない場合があります。切断処理が正常に終了できない場合に、再び同一 NQ へのネットワーク接続を行っても、正常に表示されなくなることがあります。
以下に、コマンドプロンプト使用時に現象が発生した場合の一例を示します。



『接続 2』のネットワーク接続を切断後、再接続させるため telnet コマンドを実行します（上記②を参照）。しかし、telnet コマンド実行後、『接続 2』にメッセージなどが一切出力されず、文字入力を行っても表示されなくなることがあります（上記③を参照）。
上記の例は、同一のコマンドプロンプトを使用した場合となりますが、本現象は『接続 2』のネットワーク接続を切断後、新規にコマンドプロンプトを起動させ、『接続 3』として NQ へ接続しても発生する場合があります。

本現象は、同一 NQ に対する全てのネットワーク接続を切断後、再接続を行うことで解消できる場合があります。
上記の方法で解消できない場合は、全てのネットワーク接続を切断して一定時間経過後、再接

続を行ってください。一定時間経過後も表示が正常に行われない場合は、NQ の再起動を行ってください。

■NQ に対して単一のネットワーク接続を行っている場合

NQ に対して単一のネットワーク接続を行った際に文字が正常に表示されない場合、ターミナルソフトのローカルエコー設定、改行文字の変換設定が関与している可能性があります。以下は、コマンドプロンプト、および Tera Term での設定方法となります。他のターミナルソフトを使用する場合は、Tera Term の設定方法を参照し、設定内容を確認してください。

◆ コマンドプロンプトの場合

コマンドプロンプトの場合、ローカルエコー設定が関与している可能性があります。以下の手順で telnet クライアント PC の設定を確認／変更してください。

① コマンドプロンプトを起動し、telnet コマンドを入力します。

```
C:¥> telnet
Microsoft (R) Windows 2000 (TM) Version 5.00 (Build 2195)
Microsoft Telnet クライアントへようこそ
Telnet Client Build 5.00.99206.1

エスケープ文字は 'CTRL+]' です

Microsoft Telnet>
```

引数は設定しない

② display コマンドを使用し、設定を確認します。

```
Microsoft Telnet> display
エスケープ文字は 'CTRL+]' です
自動認証 (NTLM 認証) を使う
ローカルエコーを使わない
CR と LF を送信します
使用する端末の種類をネゴシエートする

優先する端末の種類は ANSI です
Microsoft Telnet>
```

設定確認を行う

③ 入力文字が表示されていない場合は、ローカルエコーをオンにします。

```
Microsoft Telnet> set local_echo
Microsoft Telnet> display
エスケープ文字は 'CTRL+]' です
自動認証 (NTLM 認証) を使う
ローカルエコーを使う
CR と LF を送信します
使用する端末の種類をネゴシエートする

優先する端末の種類は ANSI です
Microsoft Telnet>
```

ローカルエコーを設定
設定確認を行う

※ 上記の設定を行った場合、PC の再起動後も設定が保存されています。
※ ローカルエコーの設定を戻す場合は、以下のコマンドを入力してください。

```
Microsoft Telnet> unset local_echo
```

④ telnet を終了します。

```
Microsoft Telnet> quit
```

◆ Tera Term の場合

Tera Term の場合、ローカルエコー設定、改行文字の変換設定が関与している可能性があります。以下の手順で telnet クライアント PC の設定を確認／変更してください。

[Setup] → [Terminal]

Receive	: CR	受信改行文字の変換設定
Transmit	: CR+LF	送信改行文字の変換設定
Local echo	: ON	ローカルエコー設定
Kanji(receive)	: SJIS	受信文字コード設定（EUC でも可）
Kanji(transmit)	: SJIS	送信文字コード設定

６．２　USBメモリを使用したセットアップに失敗する

USB メモリを使用したセットアップを行っても SiteManager-NQ 間の通信が正常に行えない場合、NQ が USB メモリを認識できていない、あるいは設定ファイルに記載された内容が間違っている可能性があります。USB メモリの認識状態、および設定エラーを判断するには、以下を確認してください。

NQ 起動時に USB メモリを認識した場合は、USB メモリのルートフォルダに以下のファイルが作成されます。

［ファイル名］

svconflog.txt （全て半角小文字）

［ファイル内詳細］

```
YYYY/MM/DD hh:mm:ss JST: mount ok
```

［内容］

引数	説明
YYYY/MM/DD	svconflog.txt を作成した日付
hh:mm:ss	svconflog.txt を作成した時刻
JST:	日本時間であることを示す（固定）
mount ok	認識できたことを示す（固定）

［注意］

USB メモリ内に同一ファイル名があった場合は既存ファイルを削除し、新規作成します。

本ファイルが存在しない場合、もしくはファイル内の日付や時刻が古い場合、NQ と USB メモリの相性によって USB メモリが認識できていない可能性があります。また、NQ30c は USB2.0 の USB メモリのみ使用できます。２．２．１章のセットアップ手順を実行しても認識できない場合は、USB メモリを変更して実施してください。

USBメモリの設定ファイル読み込み時にエラーが発生した場合、本ファイルに以下のエラーログを出力します。エラーログに出力される内容は、設定ファイルに記載した内容を設定するコマンドと、その実行結果（３．５　コマンド入力時の注意・制限事項参照）です。エラーログ出力時は、２．２．３章、２．２．４章の設定例、あるいは７．１章の「Password」の項目を参照し、設定ファイルの確認を行ってください。

［認証パスワード未記入］

```
YYYY/MM/DD hh:mm:ss JST: no password
```

[認証パスワードによる認証失敗]

```
YYYY/MM/DD hh:mm:ss JST: password error
```

[不正なパラメータ指定による設定失敗]

例：以下のような設定ファイルを用いて設定した場合：(DisableWatchMyNetwork:0 が不正なパラメータ)

```
password:admin
DisableWatchMyNetwork:0
DisableOtherNetworkHostPrevent:1
```

svconflog.txt に以下の内容を出力します。

```
2009/09/08 00:30:09 JST: mount ok
+ Welcome to SvNaConsole.
set na DisableWatchMyNetwork 0
- 503 invalid data.
set na DisableOtherNetworkHostPrevent 1
+ Command succeeded.
+ Goodbye.
```

６．３　NQにネットワーク設定が正常に反映されたか確認できない

２章を参照して NQ の設定を行った場合、SiteManager インストール PC と正常に通信可能で、SiteManager サービスが起動していれば、SiteManager インストール PC 上のサイトコンソールにエージェントアイコンが表示されます。
サイトコンソールに表示されない場合や SiteManager サービスが起動していない場合、下記の例を参照して NQ の設定状態を確認してください。

※ 以下の手順は、NQ に設定されている IP アドレスを把握していることを前提としています。NQ の IP アドレスが分からない場合はネットワーク接続を行うことができないため、２．２章を参照して USB メモリによる設定変更を行ってください。

① NQ を起動する

NQ 筐体へ、ネットワークに接続された LAN ケーブル、電源ケーブルを接続してください。接続完了後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。
但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下して起動してください。起動状態は、電源ランプの点灯状態から確認してください。

② telnet クライアント PC を用意する

NQ へ telnet を介してネットワーク接続を行う PC を用意し、ping コマンドなどを使用して NQ との通信状態を確認してください。

［実行例］

```
C:¥> ping 192.168.250.250 (※)
```

※ 斜体部分は NQ に設定されている IP アドレス、あるいは IP アドレスに割り当てられているホスト名を設定してください。

NQ と通信できない場合、NQ に設定されているネットワークと接続できるよう、telnet クライアント PC のネットワーク設定を変更してください。

③ NQ にネットワーク接続する

３．２章を参照し、telnet クライアント PC から NQ へネットワーク接続を行ってください。

④ 各種設定を確認する

NQ へ接続後、下記の例を参考に設定状態を確認してください。

［実行例］

```
svna> pass admin
+ Welcome to SvNaConsole.
svna> list if
= Command succeeded.
eth0    inet addr:192.168.250.250 HWaddr 00:00:4c:11:22:33
        Mask:255.255.255.0  Bcast:192.168.250.255
        Default Gateway:192.168.250.1
        UP  BROCAST  RUNNING  MULTICAST
+ Done.
svna> list ns
= Command succeeded.
nameserver 192.168.250.6
nameserver 192.168.250.7
domain isnq.dom
+ Done.
svna> list na
= Command succeeded.
AdminMailAddress: admin@securevisor.dom
…
+ Done.
svna>
```

→認証コマンドの詳細は３．６．１章参照

→ネットワークインターフェース確認
　コマンドの詳細は３．６．３章参照

→DNS ネームサーバ、ドメイン名確認
　コマンドの詳細は、３．６．４章参照

→エージェント設定確認コマンドの詳細は
　３．６．５章参照、エージェント設定の
　各属性の詳細は４章参照

６．４　SiteManagerインストールPCを不正接続防止してしまった

SiteManager インストール PC を不正接続防止した場合は、SiteManager-NQ 間の通信が正常に行えなくなり、各種操作が行えなくなります。不正接続防止機能を強制的に停止させたい場合は、下記の手順を実施してください。

① NQ を停止する

NQ の電源ケーブルを抜いて、電源を停止してください。NQ30a、NQ30c の場合は電源スイッチの長押しでも電源を停止させることができます。

② SiteManager サービスを停止する

NQ の接続先に設定されている SiteManager サービスを停止してください。サービスの停止手順は以下の通りです。

Windows の[スタート]ボタン → コントロール パネル → 管理ツール → サービス → [SecureVisor SiteManager]を選択し、サービスを停止する。

③ SiteManager の管理するエージェント設定を変更する

SiteManager が保持している NQ の属性ファイルを編集し、不正接続防止機能が無効となるよう設定します。

NQ の属性ファイルは下記の場所にあります。

C:¥Program Files¥SecureVisor¥SiteManager¥Data¥AgentList¥*xxxx*¥attribute.dat ※SiteManager を "C:¥Program Files¥SecureVisor" にインストールした場合

※ *xxxx* は、NQ のエージェント名を示します。

attribute.dat ファイルをメモ帳などのエディタで開き、不正接続防止機能（JamStatus）の属性を以下のように変更してください。

JamStatus: On

↓

JamStatus: Off

※ SiteManager の属性ファイルは、文字コードを Shift-JIS、改行コードを<CR>+<LF>で作成されています。使用するテキストエディタの設定を確認の上、編集、保存を行ってください。なお、Windows 標準のメモ帳は前述の設定を満たしているため、問題なく使用できます。

④ SiteManager のサービスを開始する

NQ の接続先に設定されている SiteManager サービスを開始してください。サービスの開

始手順は以下の通りです。

Windows の[スタート]ボタン → コントロール パネル → 管理ツール → サービス → [SecureVisor SiteManager]を選択し、サービスを開始する。

⑤NQ の設定ファイルを作成する

NQ に設定されている不正接続防止機能を停止させるため、２．２．２章、および２．２．３章を参照し、USB メモリのルートフォルダに設定ファイルを作成します。

［ファイル名］

svconfig.txt （全て半角小文字）

［設定内容］

```
Password:admin
JamStatus:Off
```

→ 認証パスワードを記述してください。
→ 不正接続防止機能を Off に設定します。

⑥NQ を起動する

NQ 筐体へ、設定ファイルを保存した USB メモリ、ネットワークに接続された LAN ケーブル、電源ケーブルが接続されていることを確認してください。接続確認後、電源ケーブルをコンセントへ差し込むことにより、自動起動します。

但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

上記手順実行後、NQ は起動時に SiteManager へ接続することで設定内容が同期され、不正接続防止機能が無効となります。

不正接続防止機能を再度有効とする場合、ホスト一覧を使用し、ネットワークへの接続を許可する機器が全て接続許可状態になっていることを確認してから設定してください。

６．５　現在のNQのバージョンが分からない

NQ のバージョンは、SiteManager インストール PC から確認することができます。確認手順は、下記の通りです。

■NQ 単位で確認する場合

1. SiteManager インストール PC で、サイトコンソールを起動します。サイトコンソールの起動方法は、以下を参照してください。

Windows の[スタート]ボタン → (すべての)プログラム → SecureVisor →サイトコンソール

2. サイトコンソールでエージェントのプロパティを選択し、エージェント設定ダイアログを起動させ、[バージョン情報]を確認してください。エージェントのプロパティ選択方法は、以下のいずれかを参照してください。

・バージョン確認対象の NQ のエージェントアイコン上で、マウスの左ボタンをクリックして選択する。選択後は、以下のいずれかを実行してください。

●メニューバーより[ファイル(F)] → [エージェントのプロパティ(P)...]を選択する

●ツールバーの左から 2 番目の[プロパティ]ボタンをクリックする

●エージェントアイコン上でマウスの左ボタンをダブルクリックする

●エージェントアイコン上で、マウスの右ボタンをクリックしてポップアップメニューを表示させ、[プロパティ(P)...]を選択する。

■複数の NQ をまとめて確認する場合

（１）サイトコンソールのメインダイアログから確認する

1. SiteManager インストール PC で、サイトコンソールを起動します。サイトコンソールの起動方法は、上記の「■NQ 単位で確認する場合」の 1. を参照してください。
2. サイトコンソールのツールバーで[表示形式の変更]ボタンをクリックする。エージェントの表示を詳細形式に切り替えると、SiteManager が管理しているエージェントの IP アドレス、バージョン情報などを一括で確認することができます。

（２）サイトコンソールのエージェント情報一覧ダイアログから確認する

1. SiteManager インストール PC で、サイトコンソールを起動します。サイトコンソールの起動方法は、上記の「■NQ 単位で確認する場合」の 1. を参照してください。
2. サイトコンソールのメニューバーより[ツール(T)] → [エージェント情報一覧(T)...]を選択する。エージェント情報一覧ダイアログが表示され、SiteManager が管理しているエージェントの IP アドレス、バージョン情報などを一括で確認することができます。

６．６　タグVLAN環境でNQが使用できない

NQ の「タグ VLAN 対応機能」を使用してトランクポートに接続しても、スイッチの設定によっては正常に動作しないことがあります。例として、Cisco Catalyst シリーズのスイッチで構築したタグ VLAN 環境で NQ を使用する場合の注意点を以下に示します。

■トランクポートにネイティブ VLAN が含まれないこと

Cisco Catalyst シリーズでは、IEEE802.1Q トランクにおいてネイティブ VLAN（Catalyst3550 では VLAN 1 が既定）を定義しています。ネイティブ VLAN は、トランクポートに設定してもタグ付けされずに転送するため、NQ にネイティブ VLAN の VLAN ID を収集対象として追加しても、タグ付きパケットでないため収集できません。

また、トランクポートにネイティブ VLAN が含まれている場合、トランクポートに接続した機器のネイティブ VLAN を一致させる必要があるため、設定によっては NQ を接続した際にエラーとなる場合があります。

Cisco Catalyst シリーズでトランクポートを設定する際は、ネイティブ VLAN を外して利用してください。

上記以外にも、使用されているスイッチ固有の設定により、正常に動作しない場合があります。使用されるスイッチのマニュアルを参照の上、適切な設定を実施して利用してください。

７．設定ファイルのパラメータ詳細

設定パラメータは、設定必須パラメータ、設定可能パラメータがあります。また、「タグ VLAN 対応機能」の設定の有無によって、使用できるパラメータが異なります。以降の説明を参照の上、設定の必要に応じて各パラメータを利用してください。

７．１　各環境共通の設定必須パラメータ

非タグ VLAN 環境、タグ VLAN 環境共通の設定必須パラメータを以下に示します。

パラメータ	説明	既定値
Password	認証パスワードを設定します。認証パスワードは、ネットワーク接続で使用する認証パスワードと共通です。 設定値は、1 個のみ記述可能です。本パラメータは、必ず設定ファイルの 1 行目に記述してください。1 行目にない場合、設定ファイルに記載された各パラメータが反映されません。 設定値に使用可能な文字は、1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。４．２．１章の注意事項を参照の上、記述してください。 なお、認証パスワードはセキュリティ対策として既定値から変更することを推奨します。認証パスワードの変更方法は、３．６．２章を参照してください。 ■記述例 Password:admin	admin
AgentName	サイトコンソールに表示するエージェント名を設定します。設定値は、1 個のみ記述可能です。 設定値は、４．３章の注意事項を参照の上、入力してください。 設定値に使用可能な文字は、半角英数字、ハイフン（-）、アンダーバー（_）、ドット（.）小括弧（(,)）からなる 1 バイト(文字)以上 32 バイト(文字)以下の文字列で、大文字、小文字は区別されません。また、以下に該当する文字列を設定した場合は、SiteManager に登録することができません。 ●Windows 予約デバイス名（AUX、CON、NUL、PRN、COM0～COM9、LPT0～LPT9） ●エージェント名の先頭、あるいは末尾がドット（.）である	isnq30

	『isnq30(1)』のように文字列の末尾に小括弧で囲んだ半角数字を記述する場合、SiteManager オンラインヘルプを参照し、サイトコンソールのエージェント設定ダイアログから行ってください。 ■記述例 AgentName:isnq30	
IpAddress	ネットワークインターフェースが使用する IP アドレスを設定します。設定値は、1 個のみ記述可能です。 設定値は、４．１章の注意事項を参照の上、記述してください。設定可能な範囲は、『1.0.0.1』～『223.255.255.254』までとなります。 NQ をタグ VLAN 環境に設置する場合、本パラメータと VLAN インターフェースに設定する IP アドレスの重複を避けるため、『127.0.0.1』を記述してください。 ■記述例 IpAddress:192.168.250.250	192.168.250.250
ManagerAddress	NQ の管理/操作を行う SiteManager インストール PC の IP アドレスを設定します。設定値は、1 個のみ記述可能です。 設定値は、４．１章の注意事項を参照の上、記述してください。 ■記述例 ManagerAddress:192.168.250.251	192.168.250.251

７．２　非タグVLAN環境の設定必須パラメータ

非タグ VLAN 環境の設定必須パラメータを以下に示します。

パラメータ	説明	既定値
NetworkMask	設置するネットワークのサブネットマスクを設定します。設定値は、1 個のみ記述可能です。 設定値は、４．１章の注意事項を参照の上、記述してください。設定可能な範囲は、『255.0.0.0』の 8 ビットから『255.255.255.252』の 30 ビットまでとなります。 ■記述例 NetworkMask:255.255.255.0	255.255.255.0

７．３　タグVLAN環境の設定必須パラメータ

タグ VLAN 環境の設定必須パラメータを以下に示します。

パラメータ	説明	既定値
Vlan1～Vlan32	「タグ VLAN 対応機能」で使用する VLAN インターフェースの設定を追加/更新します。VLAN インターフェースには、各 VLAN 内で使用可能な IP アドレスを割り当てる必要があります。各パラメータに対して、設定値を 1 組のみ記述可能です。Vlan1～Vlan8（NQ30c の場合は Vlan1～Vlan16）のパラメータを、必要数に応じて使用してください。NQ を冗長化構成で使用する場合は、Vlan1～Vlan16（NQ30c の場合は Vlan1～Vlan32）のパラメータを設定可能です。 設定値は、以下の定義に従って順に記述してください。各設定値は、半角スペースで繋いだ形式で記述してください。全ての設定値が記述されていない場合、設定が反映されません。 ●IP アドレス → ４．１章の注意事項を参照し、『1.0.0.1』～『223.255.255.254』の範囲で設定 ●サブネットマスクの有効ビット数 → 10 進数で『8』～『30』の範囲で設定 ●VLAN ID → 10 進数で『0』～『4094』の範囲で設定 設定時は、以下の点に注意してください。 ●VLAN インターフェースの設定数は、最大で 8 個（NQ30c の場合は 16 個）までのサポートとなります。 ●パラメータは、1 行目から順番に読み込まれます。VLAN ID が重複したパラメータが存在する場合、後に記述された内容に上書きされます。 ●NQ に同一 VLAN ID が設定済の場合、設定ファイルの内容に更新します。 ■記述例 Vlan1:192.168.250.251 24 1001 Vlan2:172.16.180.15 23 2001	未設定

７．４　各環境共通の設定可能パラメータ

非タグ VLAN 環境、タグ VLAN 環境共通の設定可能パラメータを以下に示します。

パラメータ	説明	既定値
ActiveNic	「NQ 冗長化機能」利用時に設定します。管理対象の VLAN ID を指定します。最大 8 個（NQ30c の場合は 16 個）まで設定可能です。設定値が指定されていない場合、管理範囲は VLAN インターフェース追加コマンドで設定しているすべての VLAN となります。「NQ 冗長化機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■記述例 ◆設定時 ActiveNic:eth0.2,eth0.3,eth0.4,eth0.5,eth0.6,eth0.7 ◆削除時 ActiveNic:””	未設定
AdminMailAddress	NQ の管理者メールアドレスを設定します。本パラメータを設定した場合、該当の NQ に関するアラートが発生し、メール送信が行われる際に、設定値がメール送信先として追加されます。設定値は、複数記述可能です。設定値に使用可能な文字は、半角英数字、ハイフン（-）、アンダーバー（_）、ドット（.）からなる 0 バイト以上 1024 バイト以下の文字列で、文字列中にアットマーク（@）をひとつ含み、アットマークの前後に 1 文字以上あるものを、正しいメールアドレスとして扱っています。また、カンマ（,）で区切ることで複数指定可能ですが、カンマの前後に空白は入力できません。なお、設定値を削除する場合、ダブルクォート（”）を使用し、『””』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例 ◆設定時 AdminMailAddress:user@securevisor.dom,admin@securevisor.dom ◆削除時 AdminMailAddress:””	未設定

AdminName	NQ の管理者氏名を設定します。本パラメータを設定した場合、SiteManager のアラート通知機能を使用する際に、メール送信、コマンド起動（SNMP トラップ送信機能含む）の通知内容に管理者氏名を含めることができます。設定値は、1 個のみ記述可能です。 設定値に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 40 バイト以下の文字列で、大文字、小文字は区別されます。４．２．２章の注意事項を参照の上、記述してください。 ■記述例 ◆設定時 AdminName:ネットワーク管理者 ◆削除時 AdminName:””	未設定
AdminPassword	認証パスワードを変更します。認証パスワードは、ネットワーク接続で使用する認証パスワードと共通です。設定値は、1 個のみ記述可能です。 設定値に使用可能な文字は、1 バイト(文字)以上 8 バイト(文字)以下の半角英数字、半角記号、半角スペースからなる文字列です。大文字、小文字を区別します。8 バイト(文字)より長い場合は、以降の文字列は認識されません。４．２．１章の注意事項を参照の上、記述してください。 ■記述例 AdminPassword:passwd	
AdminTelephoneNumber	NQ の管理者電話番号を設定します。本パラメータを設定した場合、SiteManager のアラート通知機能を使用する際に、メール送信、コマンド起動（SNMP トラップ送信機能含む）の通知内容に管理者電話番号を含めることができます。設定値は、1 個のみ記述可能です。 設定値に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 100 バイト以下の文字列で、大文字、小文字は区別されます。４．２．２章の注意事項を参照の上、記述してください。 ■記述例 ◆設定時 AdminTelephoneNumber:000-111-2222	未設定

	◆削除時 AdminTelephoneNumber:””	
AgentLocation	NQ の設置場所を設定します。本パラメータを設定した場合、SiteManager のアラート通知機能を使用する際に、メール送信、コマンド起動（SNMP トラップ送信機能含む）の通知内容に設置場所を含めることができます。設定値は、1 個のみ記述可能です。 設定値に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 255 バイト以下の文字列で、大文字、小文字は区別されます。４．２．２章の注意事項を参照の上、記述してください。 ■記述例 ◆設定時 AgentLocation:○×ビル 4F ◆削除時 AgentLocation:””	未設定
AgentPort	NQ が SiteManager からの通信を受信するポート番号を設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『1』～『65535』の範囲で記述してください。但し、telnet を介したネットワーク接続の使用ポートである『23496』は設定しないでください。 ■記述例 AgentPort:23491	23491
Charset	設定ファイルの文字コード指定を設定します。設定値は、1 個のみ記述可能です。本パラメータ使用時は、必ず設定ファイルの 2 行目に記述してください。 設定値は、Shift_JIS を指定する場合は『sjis』、日本語 EUC(EUC-JP)を指定する場合は『eucjp』を記述してください。本パラメータがない場合、設定ファイルの文字コードは Shift_JIS として処理されます。 本パラメータで指定された文字コードと、設定ファイルの文字コードが異なる場合、全角文字を反映させることができません。 ■記述例 Charset:eucjp	sjis
CheckHttpPort	「承認申請機能」利用時に設定します。不正接続防止された端末から HTTP アクセスによる承認申請要求を許	80

	可する TCP ポート番号を指定します。最大 32 個まで設定可能です。設定値は、10 進数で『1』～『65535』の範囲で記述してください。複数のポート番号を記述する場合、カンマ（,）で区切って記述してください。 「承認申請機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■記述例 CheckHttpPort:80,8080,8081,8082,8031	
CollectOfPacket	データ収集の有効/無効を設定します。設定値は、1 個のみ記述可能です。設定値は、収集を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 ■記述例 CollectOfPacket:On	Off
ContinuePrevention	「Gratuitous ARP 非準拠機器対応機能」を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。 「Gratuitous ARP 非準拠機器対応機能」については、９．３章を参照してください。 ■記述例 ContinuePrevention:On [注意事項] DisableBroadCastJamArp の設定値を『1』（偽装 ARP パケットの送信方式がユニキャスト）にする場合は、ContinuePrevention の設定値を『Off』にしてください。	Off
DefaultGateway	NQ を設置するネットワークのデフォルトゲートウェイアドレスを設定します。設定値は、1 個のみ記述可能です。 設定値は、４．１章の注意事項を参照の上、記述してください。 ■記述例 DefaultGateway:192.168.250.1	192.168.250.1
DefaultGateway(-)	NQ に設定されているネットワークのデフォルトゲートウェイアドレスを削除します。設定値は 1 個のみ記述可	

	能です。 設定値は、アスタリスク（*）を記述してください。 ■記述例 DefaultGateway(-):*	
DhcpScope	NQ が監視するネットワークで設定されている DHCP スコープの範囲を設定します。設定値は、32 個まで記述可能です。 本パラメータは、NQ が管理しているホストの IP アドレスが固定 IP アドレス、DHCP クライアントのどちらかを判断する場合に利用します。 ここで指定した範囲内の IP アドレスを検知した場合、"DHCP クライアント"と判断します。なお、サイトコンソールの[ホスト一覧設定ダイアログ]で設定する同一ホストとみなす条件で「プロトコルアドレス」を選択している場合、発見したホストの IP アドレスが DHCP スコープの範囲内であれば 新規ホストではなく既存ホストの更新となる場合があります。 設定値は、『10.0.0.2-10.0.0.9』のように、開始と終了の IP アドレスは４．１章の注意事項を参照の上、記述してください。開始アドレスと終了アドレスの間は、ハイフン（-）で繋いだ形式で記述してください。複数の DHCP スコープを記述する場合、半角スペースで繋いだ形式で記述してください。 本パラメータを使用した場合、以前の設定内容を破棄して設定値を反映させます。設定値を削除する場合、ダブルクォート（"）を使用し、『""』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■記述例 ◆設定時 DhcpScope:10.0.0.1-10.0.0.5 10.0.0.7-10.0.0.9 ◆削除時 DhcpScope:""	未設定
DisableBroadCastJamArp	偽装 ARP パケットの送信方式を指定します。設定値は、1 個のみ記述可能です。設定値は、『0』あるいは『1』を記述してください。『0』の場合はブロードキャスト、『1』の場合はユニキャストとなります。 設定値が『1』の場合、以下の現象の回避策が有効になります。 ・DHCP クライアントの MacOS 端末を不正接続防止すると、Mac OS 端末が IP アドレスの取得を繰り返し DHCP サーバのアドレスプールが枯渇する。	0

	・承認済みの Windows Vista 以降の端末と未承認の端末との間の通信が防止されない。 ■記述例 DisableBroadCastJamArp:1 [注意事項] DisableBroadCastJamArp の設定値を『1』(偽装 ARP パケットの送信方式がユニキャスト)にする場合は、ContinuePrevention の設定値を『Off』にしてください。	
DisablePreventionAutoIPAddr	固定 IP アドレスを設定している Windows Vista などを不正接続防止すると APIPA により自動的に新しいアドレスが割り振られ、さらにその IP アドレスを不正接続防止するということを繰り返し、大量のホスト情報の表示および、防止通知が行われる場合があります。本機能は、APIPA などに代表される AutoIP アドレスとして割り振られる LINKLOCAL アドレス(169.254.0.0/16)を持つホストを不正接続防止から除外する機能です。 On:AutoIP アドレス防止除外機能が有効 Off:AutoIP アドレス防止除外機能が無効 ■記述例 DisablePreventionAutoIPAddr:On	Off
DisablePreventionWhenNotConnectSM	SiteManager と通信できない場合に、不正接続防止機能を有効/無効にする機能を設定します。設定値は、1 個のみ記述可能です。 設定値は、通信不可時も不正接続防止機能を有効とする場合は『0』、無効とする場合は『1』を設定してください。 ただし、NQ を再起動した場合はメモリ内の承認ポリシーが消去されるため、設定値が『0』の場合でも、SiteManager から承認ポリシーを取得できるまで不正接続防止機能は有効になりません。 ■記述例 DisablePreventionWhenNotConnectSM:0	1
DisableUnicastJamArp	特定条件において承認済みの Windows Vista 以降の端末のネットワークインターフェースが無効になる現象を	0

	回避させる機能の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。 詳細は、「SecureVisor Ver3.8 注意制限事項」を参照してください。 ■記述例 DisableUnicastJamArp:0	
DNSServer	NQ を設置するネットワークで使用されている DNS サーバの IP アドレスを設定します。設定値は、3 個まで記述可能です。 設定値に IP アドレスを記述する場合、４．１章の注意事項を参照の上、記述してください。また、設定値を 2～3 個記述する場合、半角スペースで繋いだ形式で記述してください。 本パラメータを使用した場合、以前の設定内容を破棄して設定値を反映させるため、DNS サーバの削除パラメータ（DNSServer(-)）の設定は不要です。 ■記述例 DNSServer:192.168.250.6 192.168.250.7	未設定
DNSServer(-)	NQ に設定されている DNS サーバの IP アドレスを削除します。設定値は、3 個まで記述可能です。 設定値に IP アドレスを記述する場合、４．１章の注意事項を参照の上、記述してください。IP アドレスが記述された場合、一致する設定のみ削除します。また、設定値を 2～3 個記述する場合、各 IP アドレスを半角スペースで繋いだ形式で記述してください。 設定値にアスタリスク（*）のみ記述した場合、全ての設定を削除します。 なお、設定値に IP アドレスとアスタリスクを併用して記述されている場合、削除処理が行われません。 ■記述例 ◆指定削除時 DNSServer(-):192.168.250.6 192.168.250.7 ◆一括削除時 DNSServer(-):*	
DomainName	NQ を設置するネットワークのドメイン名を設定します。設定値は、複数記述可能です。 設定値は、ネットワークのドメイン名を記述してください。複数のドメイン名を記述する場合、半角スペースで繋いだ形式で記述してください。設定可能な文字数の合計は 2,000 文字です。文字数制限には、複数設定時	isnq.dom

	に引数の間に設定する半角スペースも含まれます。 ■記述例 DomainName:isnq.dom test.dom	
DomainName(-)	NQ に設定されているネットワークのドメイン名を削除します。設定値は、複数記述可能です。 設定値をドメイン名で記述した場合、一致する設定のみ削除します。複数のドメイン名を記述する場合、半角スペースで繋いだ形式で記述してください。設定可能な文字数の合計は 2,000 文字です。文字数制限には、複数設定時に引数の間に設定する半角スペースも含まれます。 設定値をアスタリスク（*）のみで記述した場合、全ての設定を削除します。 なお、設定値にドメイン名とアスタリスクを併用して記述されている場合、削除処理が行われません。 ■記述例 ◆指定削除時 DomainName(-):isnq.dom test.dom ◆一括削除時 DomainName(-):*	
DontNotifyMacOnlyEntry	MAC アドレスしか収集できないホスト情報をホスト一覧に表示させないよう設定します。設定値は、1 個のみ記述可能です。 設定値は、MAC アドレスのみのホスト情報を表示させる場合は『0』、表示させない場合は『1』を設定してください。 ■記述例 DontNotifyMacOnlyEntry:1	0
ExceptMacVendor	特定ベンダの MAC アドレスを不正接続防止対象から除外する機能の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。 Ver3.8 では、Apple 社の MAC アドレス(IEEE-SA にて 2011 年 7 月 中旬に登録が確認されたもの)が不正接続防止対象から除外されるよう定義されています。 ■記述例	0

	ExceptMacVendor:0	
FailOverMode	「NQ 冗長化機能」利用時に設定します。NQ の「冗長化モード」を設定します。設定値は、1 個のみ記述可能です。『On』の場合は「アクティブ」、『Off』の場合は「スタンバイ」になります。 「NQ 冗長化機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■記述例 FailOverMode:On	On
Ifspeed	NQ のネットワークインターフェースのネゴシエーション設定を変更します。設定値は、1 個のみ記述可能です。設定値は、オートネゴシエーションは『auto』、100base-Tx 全二重通信は『100FD』、100base-Tx 半二重通信は『100HD』、10base-T 全二重通信は『10FD』、10base-T 半二重通信は『10HD』を記述してください。 ■記述例 Ifspeed:100FD	auto
JamMacAddressMode	偽装 ARP パケットのアドレスモードを指定します。設定値は、1 個のみ記述可能です。設定値は、『0』あるいは『1』を記述してください。『1』の場合は以下の機能を有効にするモードとなります。 ・承認申請機能 ・承認済みの Windows Vista 以降の端末と未承認の端末との間の通信が防止されない現象の回避策 「承認申請機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■記述例 JamMacAddressMode:1	0
JamStatus	NQ の不正接続防止機能を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。サイトコンソールに新規登録した際は、必ず『Off』が設定されます。 不正接続防止機能は、NQ の設定内容より SiteManager、あるいは集中管理画面の設定が優先されます。通常時の設定変更は、本パラメータを使用せず、サイトコンソール、または集中管理画面から行ってください。 ■記述例	Off

	JamStatus:Off	
ManagerPort	NQ が SiteManager への通信を送信するポート番号を設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『1』～『65535』の範囲で記述してください。設定値が SiteManager に設定されている受信ポート番号と異なる場合は、SiteManager と通信できなくなるため、注意してください。なお、SiteManager の受信ポート番号の変更方法は、SiteManager インストールマニュアルを参照してください。 ■記述例 ManagerPort:23490	23490
MultiNetwork	「共有ネットワーク対応機能」を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を有効にする場合は『On』、無効にする場合は『Off』を記述してください。なお、VLAN 環境設置時は、必ず本設定を無効にしてください。 ■記述例 MultiNetwork:On [注意事項] 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、本属性を On に設定してもサイトコンソールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないワーム感染ホストを防止することはできません。	Off
NetworkList NetworkList1 ～ NetworkList31	共有ネットワーク対応機能の個別指定モード(※)で、監視対象とするネットワークのアドレスとサブネットマスクを設定します。最大 31 個まで設定可能です。設定値は、ネットワークアドレスとサブネットマスクをスラッシュ(/)で区切って記述してください。サブネットマスクは 8 から 30 まで指定可能です。 (※)SiteManager オンラインヘルプの[その他の機能]－[共有ネットワーク対応機能]を参照してください。 ■記述例 NetworkList:192.168.10.0/24 NetworkList1:192.168.20.0/24 NetworkList2:192.168.30.0/24	未設定
NetworkList(-)	共有ネットワーク対応機能の個別指定モードで、監視対象とするネットワークをネットワークリストから削除	

	します。設定値は、特定のネットワークを削除する場合は、ネットワークアドレスとサブネットマスクをスラッシュ(/)で区切って記述してください。サブネットマスクは 8 から 30 まで指定可能です。監視対象ネットワークリストを空にする場合はアスタリスク（*）を指定してください。 なお、特定のネットワークを複数同時に削除することはできません。この設定値を設定ファイルに複数記述した場合、最後に記述したもののみ有効になります。 ■記述例 ◆特定のネットワークを削除する場合 NetworkList(-):192.168.10.0/24 ◆全ネットワークを削除する場合 NetworkList(-):*	
NotifyInterval	NQ が SiteManager にホスト情報の通知を行うインターバルを秒単位で設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『30』～『3600』の範囲で記述してください。 ■記述例 NotifyInterval:30	60
OsDetect	「OS デテクト機能」の有効/無効を設定します。設定値は、1 個のみ記述可能です。 設定値は、機能を無効にする場合は『0』、有効にする場合は『1』を設定してください。 「OS デテクト機能」の詳細は、SiteManager オンラインヘルプを参照してください。 ■記述例 OsDetect:0	1
PreventionTimeForYellowHost	黄で Windows と判断されたホストを発見後、接続防止を開始するまでの時間を秒単位で設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『1800』～『21600』の範囲で記述してください。 ■記述例 PreventionTimeForYellowHost:3600	3600
ProtectHost	Gratuitous ARP 非準拠機器の IP アドレスを設定します。設定値は、32 個まで記述可能です。	未設定

	設定値の IP アドレスは、４．１章の注意事項を参照の上、記述してください。複数の IP アドレスを記述する場合、カンマ（,）で区切って記述してください。設定値を削除する場合、ダブルクォート（”）を使用し、『””』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 「Gratuitous ARP 非準拠機器対応機能」については、９．３章を参照してください。 ■記述例 ◆設定時 ProtectHost:192.168.250.252,192.168.250.253 ◆削除時 ProtectHost:””	
SendArpDelay	不正アクセスの検知後に偽装 ARP パケットを送信してから再送するまでの秒数を指定します。設定値は、1 個のみ記述可能です。設定値は、10 進数で『0』～『60』の範囲で記述してください。設定値が 0 もしくは指定されない場合、本機能は無効になります。 Linux 系 OS 等、ARP エントリ更新のロックタイムが設定されている OS において、ARP エントリの偽装を有効にするために本機能を使用します。本パラメータの設定値を OS のロックタイムより長い秒数にすることで ARP エントリの偽装が有効になります。 ■記述例 SendArpDelay:1	未設定
TimeOut	通信処理時のタイムアウト時間を秒単位で設定します。設定値は、1 個のみ記述可能です。 設定値は、10 進数で『10』～『360』の範囲で記述してください。 通常は既定値で問題ありませんが、SiteManager-NQ 間の通信速度が遅い場合や、SiteManager インストール PC のマシンスペックが低い場合は、本パラメータの設定値を大きくすることで通信エラーが改善されることがあります。 ■記述例 TimeOut:20	20
Vlan(-)	設定されている VLAN インターフェースを削除します。設定値は、1 個のみ記述可能です。	

	VLAN インターフェースを指定して削除する場合、該当の VLAN インターフェースに設定されている VLAN ID を 10 進数で記述してください。全ての VLAN インターフェースを削除する場合、アスタリスク（*）を記述してください。 本パラメータを使用してタグ VLAN 環境から非タグ VLAN 環境での使用に切り替える場合、５章の制限事項を参照してください。 ■記述例 Vlan(-):101	

８．エージェント属性の確認・設定コマンドの詳細

エージェント属性の確認、および設定が可能な項目を説明します。属性項目を変更する場合、エージェント停止コマンド（３．６．２５章）実行後に実施してください。設定後はエージェント開始コマンド（３．６．２４章)、あるいは再起動コマンド（３．６．１３章）を実施してください。

※ 設定情報を確認するには、エージェント設定確認コマンド（３．６．５章）を参照してください。

※ エージェント設定確認コマンドを実行した際に非表示となる属性は、VLAN インターフェースの設定状態、あるいは属性値が未設定であることが原因となります。VLAN インターフェースの設定が影響を及ぼす属性は、８．１章を参照してください。その他の属性は、未設定の場合は既定値で動作しています。各属性の既定値は、８．２章を参照してください。

※ 設定情報を変更するには、エージェント設定コマンド（３．６．８章)、および本章の各属性に対する説明欄の入力例を参照してください。

※ 本章に記載されていない属性は、未サポートとなります。

８．１　確認のみ可能な属性の詳細

確認のみ可能な属性を以下に示します。

属性名 [attribute]	説明	既定値 [value]
IpAddress	NQ のネットワークインターフェースに設定されている IP アドレスです。VLAN インターフェースが設定されている場合、本属性は非表示となります。 属性値は、ネットワークインターフェース設定コマンド（３．６．７章参照）で変更した内容が、NQ の再起動（エージェントの停止/開始）を行った際に自動で設定されます。	192.168.250.250
CollectIpAddress	NQ が SiteManager との通信に使用する IP アドレスです。VLAN インターフェースが設定されている場合、本属性は非表示となります。 属性値は、ネットワークインターフェース設定コマンド（３．６．７章参照）で変更した内容が、NQ の再起動（エージェントの停止/開始）を行った際に自動で設定されます。	192.168.250.250
NetworkMask	NQ のネットワークインターフェースに設定されているサブネットマスクをビットマスクに変換した値です。VLAN インターフェースが設定されている場合、本属性は非表示となります。 属性値は、ネットワークインターフェース設定コマンド（３．６．７章参照）で変更した内容が、NQ の再起動（エージェントの停止/開始）を行った際に自動で設定されます。	24
NetworkAddress	NQ のネットワークインターフェースに設定されているネットワークアドレスです。VLAN インターフェースが設定されている場合、本属性は非表示となります。 属性値は、ネットワークインターフェース設定コマンド（３．６．７章参照）で変更した内容が、NQ の再起動（エージェントの停止/開始）を行った際に自動で設定されます。	192.168.250.0
NetworkList	監視対象ネットワークリストです。 属性値は、ネットワークリスト追加コマンド（３．６．２９章参照）、ネットワークリスト削除コマンド（３．６．３０章参照）で設定可能です。	未設定
NewHostStatus	NQ が新規に発見したホストをどの状態(色)で SiteManager に登録するかを示す値です。 0：新規ホストの状態(色)を「青」として登録します。 1：新規ホストの状態(色)を「黄」として登録します。 2：新規ホストの状態(色)を「赤」として登録します。	0

８．２　確認、および変更が可能な属性の詳細

確認、および変更が可能な属性を以下に示します。

属性名 [attribute]	説明	既定値 [value]
ActiveNic	「NQ 冗長化機能」利用時に設定します。管理対象の VLAN ID を指定します。最大 8 個（NQ30c の場合は 16 個）まで設定可能です。設定値が指定されていない場合、管理範囲は VLAN インターフェース追加コマンドで設定しているすべての VLAN となります。「NQ 冗長化機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■入力例 ◆設定時 set na ActiveNic eth0.2,eth0.3,eth0.4,eth0.5,eth0.6,eth0.7 ◆削除時 set na ActiveNic ""	未設定
AdminMailAddress	NQ の管理者メールアドレスです。本属性値の使用用途は、７．４章の「AdminMailAddress」の項目を参照してください。 属性値は、1 個のみ入力可能です。属性値を変更する際に使用可能な文字は、半角英数字、ハイフン（-)、アンダーバー（_)、ドット（.）からなる 0 バイト以上 1024 バイト以下の文字列で、文字列中にアットマーク（@）をひとつ含み、アットマークの前後に 1 文字以上あるものを、正しいメールアドレスとして扱っています。また、カンマ（,）で区切ることで複数指定可能ですが、カンマの前後に空白は入力できません。 ■入力例 ◆設定時 set na AdminMailAddress user@securevisor.dom,admin@securevisor.dom ◆削除時	未設定

	set na AdminMailAddress ""	
AdminName	NQ の管理者氏名です。本属性値の使用用途は、７．４章の「AdminName」の項目を参照してください。 属性値は、1 個のみ入力可能です。属性値を変更する際に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 40 バイト以下の文字列で、大文字、小文字は区別されます。４．２．２章の注意事項を参照の上、入力してください。本属性を使用する場合、telnet クライアント PC が使用する文字コードの設定に合わせて、文字コード指定コマンド（３．６．２８章参照）を使用してください。 ■入力例 ◆設定時 set na AdminName ネットワーク管理者 ◆削除時 set na AdminName ""	未設定
AdminTelephoneNumber	NQ の管理者電話番号です。本属性値の使用用途は、７．４章の「AdminTelephoneNumber」の項目を参照してください。 属性値は、1 個のみ入力可能です。属性値を変更する際に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 100 バイト以下の文字列で、大文字、小文字は区別されます。４．２．２章の注意事項を参照の上、入力してください。本属性を使用する場合、telnet クライアント PC が使用する文字コードの設定に合わせて、文字コード指定コマンド（３．６．２８章参照）を使用してください。 ■入力例 ◆設定時 set na AdminTelephoneNumber 000-111-2222 ◆削除時 set na AdminTelephoneNumber ""	未設定
AgentLocation	NQ の設置場所です。本属性値の使用用途は、７．４章の「AgentLocation」の項目を参照してください。 属性値は、1 個のみ入力可能です。属性値を変更する際に使用可能な文字は、半角英数字、半角記号文字、2 バイト文字、半角スペースからなる 0 バイト以上 255 バイト以下の文字列で、大文字、小文字は区別されます。４．２．２章の注意事項を参照の上、入力してください。本属性を使用する場合、telnet クライアント PC が使用する文字コードの設定に合わせて、文字コード指定コマンド（３．６．２８章参照）を使用してください。	未設定

	■入力例 ◆設定時 set na AgentLocation ″○×ビル 4F″ ◆削除時 set na AgentLocation ″″	
AgentName	NQ のエージェント名です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、４．３章の注意事項を参照の上、入力してください。エージェント名設定コマンド（３．６．１５章）でも設定可能です。 ■入力例 set na AgentName isnq30	isnq30
CheckHttpPort	「承認申請機能」利用時に設定します。不正接続防止された端末から HTTP アクセスによる承認申請要求を許可する TCP ポート番号を指定します。最大 32 個まで設定可能です。設定値は、10 進数で『1』～『65535』の範囲で記述してください。複数のポート番号を記述する場合、カンマ（,）で区切って記述してください。 「承認申請機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■入力例 set na CheckHttpPort 80,8080,8081,8082,8031	80
CollectOfPacket	NQ のデータ収集の設定状態です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、データ収集を開始する場合は『On』、停止する場合は『Off』を入力してください。 なお、NQ を SiteManager へ新規登録した場合は、サイトコンソール、あるいは集中管理画面より収集開始を行わなければ SiteManager と正常に通信できません。新規登録時は本コマンドから設定を変更しないでください。 ■入力例 set na CollectOfPacket Off	Off
ContinuePrevention	「Gratuitous ARP 非準拠機器対応機能」の設定状態です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、機能を有効にする場合は『On』、無効にする場合は	Off

	『Off』を入力してください。 「Gratuitous ARP 非準拠機器対応機能」については、９．３章を参照してください。 ■入力例 set na ContinuePrevention On [注意事項] DisableBroadCastJamArp の設定値を『1』（偽装 ARP パケットの送信方式がユニキャスト）にする場合は、ContinuePrevention の設定値を『Off』にしてください。	
DhcpScope	NQ が監視するネットワークで設定されている DHCP スコープの範囲です。DHCP スコープの説明は、７．４章の「DhcpScope」の項目を参照してください。 属性値は、32 個まで入力可能です。属性値を変更する際は、『10.0.0.2-10.0.0.9』のように、開始と終了の IP アドレスは４．１章の注意事項を参照の上、入力してください。開始アドレスと終了アドレスの間は、ハイフン（-）で繋いだ形式で入力してください。複数の DHCP スコープを入力する場合、ダブルクォート（″）、またはシングルクォート（'）で入力値を囲み、各 DHCP スコープの間を半角スペースで繋いだ形式で入力してください。 本属性を使用した場合、以前の設定内容を破棄して属性値を反映させます。属性値を削除する場合、ダブルクォート（″）を使用し、『″″』を記述してください。ダブルクォートの間は、スペースなどを記述しないでください。 ■入力例 ◆設定時 set na DhcpScope ″10.0.0.1-10.0.0.2 10.0.0.3-10.0.0.4″ ◆削除時 set na DhcpScope ″″	未設定
DisableBroadCastJamArp	偽装 ARP パケットの送信方式を指定します。設定値は、1 個のみ記述可能です。設定値は、『0』あるいは『1』を記述してください。『0』の場合はブロードキャスト、『1』の場合はユニキャストとなります。 設定値が『1』の場合、以下の現象の回避策が有効になります。 ・DHCP クライアントの MacOS 端末を不正接続防止すると、Mac OS 端末が IP アドレスの取得を繰り返し DHCP	0

	サーバのアドレスプールが枯渇する。 ・承認済みの Windows Vista 以降の端末と未承認の端末との間の通信が防止されない。 ■入力例 set na DisableBroadCastJamArp 1 [注意事項] DisableBroadCastJamArp の設定値を『1』（偽装 ARP パケットの送信方式がユニキャスト）にする場合は、ContinuePrevention の設定値を『Off』にしてください。	
DisableOtherNetworkHostPrevent	監視対象ネットワークリストに属さないホストを防止しないようにする機能の設定状態です。 属性値は、1 個のみ入力可能です。 0：監視対象ネットワークに属さないホストを防止しない機能が無効 1：監視対象ネットワークに属さないホストを防止しない機能が有効 ■入力例 set na DisableOtherNetworkHostPrevent 0	0
DisablePreventionAutoIPAddr	固定 IP アドレスを設定している Windows Vista などを不正接続防止すると APIPA により自動的に新しいアドレスが割り振られ、さらにその IP アドレスを不正接続防止するということを繰り返し、大量のホスト情報の表示および、防止通知が行われる場合があります。本機能は、APIPA などに代表される AutoIP アドレスとして割り振られる LINKLOCAL アドレス(169.254.0.0/16)を持つホストを不正接続防止から除外する機能です。 On：AutoIP アドレス防止除外機能が有効 Off：AutoIP アドレス防止除外機能が無効 ■入力例 set na DisablePreventionAutoIPAddr On	Off

DisablePreventionWhenNotConnectSM	SiteManager との通信不可の際に、不正接続防止機能を有効/無効とする機能の設定状態です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、通信不可時も不正接続防止機能を有効とする場合は『0』、無効とする場合は『1』を入力してください。 ただし、NQ を再起動した場合はメモリ内の承認ポリシーが消去されるため、設定値が『0』の場合でも、SiteManager から承認ポリシーを取得できるまで不正接続防止機能は有効になりません。 ■入力例 set na DisablePreventionWhenNotConnectSM 0	1
DisableUnicastJamArp	特定条件において承認済みの Windows Vista 端末のネットワークインターフェースが無効になる現象を回避させる機能の設定状態です。属性値は、1 個のみ入力可能です。 属性値を変更する際は、機能を無効にする場合は『0』、有効にする場合は『1』を入力してください。 詳細は、「SecureVisor Ver3.8 注意制限事項」を参照してください。 ■入力例 set na DisableUnicastJamArp 0	0
DisableWatchMyNetwork	監視対象ネットワークリストの InterSec/NQ30 と同一のネットワークを無視する機能の設定状態です。 On に設定した場合、同一ネットワークを監視対象外のネットワークとして扱います。属性値は、1 個のみ入力可能です。 ■入力例 set na DisableWatchMyNetwork On [注意事項] ・MultiNetwork が On の場合、及びタグ VLAN 対応機能を使用している場合は本属性を On に設定しても機能しません。 ・分散管理モードでワーム感染ホストの接続防止機能を使用する場合、本属性を On に設定しても InterSec/NQ30 と同一のネットワークでワームに感染したホストに対して不正接続防止が行われます。	Off
DontNotifyMacOnlyEntry	MAC アドレスしか収集できないホスト情報をホスト一覧に表示させない機能の設定状態です。	0

	属性値は、1 個のみ入力可能です。属性値を変更する際は、MAC アドレスのみのホスト情報を表示させる場合は『0』、表示させない場合は『1』を入力してください。 ■入力例 set na DontNotifyMacOnlyEntry 0	
ExceptMacVendor	特定ベンダの MAC アドレスを不正接続防止対象から除外する機能の設定状態です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、機能を無効にする場合は『0』、有効にする場合は『1』を入力してください。 Ver3.8 では、Apple 社の MAC アドレス(IEEE-SA にて 2011 年 7 月 中旬に登録が確認されたもの)が不正接続防止対象から除外されるよう定義されています。 ■入力例 set na ExceptMacVendor 0	0
FailOverMode	「NQ 冗長化機能」利用時に設定します。NQ の「冗長化モード」を設定します。設定値は、1 個のみ記述可能です。『On』の場合は「アクティブ」、『Off』の場合は「スタンバイ」になります。 「NQ 冗長化機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■入力例 set na FailOverMode On	On
JamMacAddressMode	偽装 ARP パケットのアドレスモードを指定します。設定値は、1 個のみ記述可能です。設定値は、『0』あるいは『1』を記述してください。『1』の場合は以下の機能を有効にするモードとなります。 ・承認申請機能 ・承認済みの Windows Vista 以降の端末と未承認の端末との間の通信が防止されない現象の回避策 「承認申請機能」の詳細は、「SecureVisor Ver3.8 集中管理運用マニュアル」を参照してください。 ■入力例 set na JamMacAddressMode 1	0
JamStatus	NQ の不正接続防止機能の設定状態です。	Off

	属性値は、1個のみ入力可能です。属性値を変更する際は、機能を有効にする場合は『On』、無効にする場合は『Off』を入力してください。 不正接続防止機能は、NQの設定内容よりSiteManager、あるいは集中管理画面の設定が優先されます。通常時の設定変更は、本属性を使用せず、サイトコンソール、または集中管理画面から行ってください。 ■入力例 set na JamStatus Off	
ManagerIpAddress	NQの管理/操作を行うSiteManagerインストールPCのIPアドレスです。 属性値は、1個のみ入力可能です。属性値を変更する際は、４．１章の注意事項を参照の上、入力してください。マネージャ設定コマンド（３．６．１４章）でも設定可能です。 ■入力例 set na ManagerIpAddress 192.168.250.251	192.168.250.251
ManagerPort	NQがSiteManagerへの通信を送信するポート番号です。 属性値は、1個のみ入力可能です。属性値を変更する際は、10進数で『1』～『65535』の範囲で入力してください。属性値がSiteManagerに設定されている受信ポート番号と異なる場合は、SiteManagerと通信できなくなるため、注意してください。なお、SiteManagerの受信ポート番号変更方法は、SiteManagerインストールマニュアルを参照してください。 ■入力例 set na ManagerPort 23490	23490
MultiNetwork	「共有ネットワーク対応機能」の設定状態です。 属性値は、1個のみ入力可能です。属性値を変更する際は、機能を有効にする場合は『On』、無効にする場合は『Off』を入力してください。 ■入力例 set na MultiNetwork On [注意事項] 分散管理モードでワーム感染ホストの接続防止機能を使用する場合、本属性をOnに設定してもサイトコンソ	Off

	ールのエージェント設定ダイアログに表示される監視対象ネットワークリストに属さないワーム感染ホストを防止することはできません。	
NotifyInterval	NQ が SiteManager にホスト情報の通知を行うインターバルです。属性値の単位は秒です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、10 進数で『30』～『3600』の範囲で入力してください。 ■入力例 set na NotifyInterval 30	60
OsDetect	「OS デテクト機能」の設定状態です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、OS デテクト機能を無効にする場合は『0』、有効にする場合は『1』を入力してください。 「OS デテクト機能」の詳細は、SiteManager オンラインヘルプを参照してください。 ■入力例 set na OsDetect 0	1
Port	NQ が SiteManager からの通信を受信するポート番号です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、10 進数で『1』～『65535』の範囲で入力してください。但し、ネットワーク接続の使用ポートである『23496』は設定しないでください。 ■入力例 set na Port 23491	23491
PreventionTimeForYellowHost	黄で Windows と判断されたホストを発見後、接続防止を開始するまでの時間です。属性値の単位は秒です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、10 進数で『1800』～『21600』の範囲で入力してください。 ■入力例 set na PreventionTimeForYellowHost 3600	3600
ProtectHost	Gratuitous ARP 非準拠機器の IP アドレスです。 属性値は、32 個まで入力可能です。属性値を変更する際は、４．１章の注意事項を参照の上、IP アドレスを入力してください。複数の IP アドレスを入力する場合、カンマ（,）で区切って入力してください。設定値を	未設定

	削除する場合、ダブルクォート（″）を使用し、『″″』を入力してください。ダブルクォートの間は、スペースなどを入力しないでください。 「Gratuitous ARP 非準拠機器対応機能」については、９．３章を参照してください。 ■入力例 ◆設定時 set na ProtectHost 192.168.250.252,192.168.250.253 ◆削除時 set na ProtectHost ″″	
SendArpDelay	不正アクセスの検知後に偽装 ARP パケットを送信してから再送するまでの秒数を指定します。設定値は、1 個のみ記述可能です。設定値は、10 進数で『0』～『60』の範囲で記述してください。設定値が 0 もしくは指定されない場合、本機能は無効になります。 Linux 系 OS 等、ARP エントリ更新のロックタイムが設定されている OS において、ARP エントリの偽装を有効にするために本機能を使用します。本パラメータの設定値を OS のロックタイムより長い秒数にすることで ARP エントリの偽装が有効になります。 ■入力例 set na SendArpDelay 1	未設定
TimeOut	通信処理時のタイムアウト時間です。属性値の単位は秒です。 属性値は、1 個のみ入力可能です。属性値を変更する際は、10 進数で『10』～『360』の範囲で入力してください。 通常は既定値で問題ありませんが、SiteManager-NQ 間の通信速度が遅い場合や、SiteManager インストール PC のマシンスペックが低い場合は、本属性の属性値を大きくすることで通信エラーが改善されることがあります。 ■入力例 set na TimeOut 20	20

９．HowTo集

９．１　NQの時刻をSiteManagerと同期させるには？

NQはSiteManagerとの同期の際に自動的に、SiteManager側のOSの時刻と同期を行っているため、時刻同期コマンド（SvNqSetTime.exe）を使用して時刻同期を行う必要はありません。
NQとSiteManagerとの同期は以下のタイミングで行います。

- NQ起動時
- NQ起動後１時間毎
- サイトコンソール上での操作（データ収集の開始/停止、新規ホストの状態（色）の設定、エージェント設定ダイアログで[OK]ボタンクリック時、不正接続防止機能の有効/無効）の１分後
- DomainManagerからNQのデータ収集の開始/停止、不正接続防止機能の有効/無効の操作の１分後（集中管理モードの場合）

９．２　通信頻度の少ない機器を検出するには？

データ収集機能はパケットモニタリング型で行われるため、通常時に自らARPリクエストを送信することのない（または少ない）ホストの検出が困難となります。接続ホスト検出促進機能を使用した場合、SiteManagerインストールPCからNQにtelnetを介して接続し、指定されたIPアドレスの範囲に対してpingを実行することで、ネットワークに接続されているホストの検出を促進させることができます。
接続ホスト検出促進機能の利用方法は、SiteManager オンラインヘルプの目次より、[SecureVisor]->[SecureVisor その他の機能]->[接続ホスト検出促進機能] を参照してください。

９．３　不正接続端末から監視対象セグメント外への通信を防止できない場合は？

ルータやスイッチなど、LAN 内の接続対象が Gratuitous ARP(※)に対応していない場合、不正接続端末の通信を防止できない場合があります。ルータやスイッチを経由した通信などが防止できない場合、「Gratuitous ARP 非準拠機器対応機能」を有効に設定し、ルータなどの IP アドレスを登録後、防止できるか確認してください。なお、本機能を有効にしている場合、特定条件において承認済みの Windows Vista 以降の端末のネットワークインターフェースが無効になる現象の回避策を有効にすることができません。現象の詳細は、「SecureVisor Ver3.8 注意制限事項」を参照してください。

(※)Gratuitous ARP については SiteManager オンラインヘルプの[SecureVisor]->[その他]->[用語集]->[Gratuitous ARP]を参照してください。

■USB メモリを使用して設定ファイルを反映させる場合
７．４章の「ContinuePrevention」、および「ProtectHost」の内容を参照し、設定ファイルに記述の上、２．２章の設定を行ってください。

■telnet による設定を行う場合
８．２章の「ContinuePrevention」、および「ProtectHost」の内容を参照し、エージェント設定コマンド（３．６．８章参照）を使用して設定を行ってください。

■SiteManager インストール PC 上からコマンドによる設定を行う場合
SiteManager オンラインヘルプの目次より、[SecureVisor]->[その他]->[HowTo 集]を選択し、「■Gratuitous ARP 非準拠機器へ対応するには？」を参照してください。

９．４　使用中のNQのエージェント名、IPアドレスを変更する方法

エージェント名や IP アドレスを変更する手順は、運用モードにより異なります。以下を参照し、利用する運用モードに応じた手順で変更してください。

９．４．１　分散管理モードの場合

９．４．１．１　エージェント名を変更する手順

エージェント名設定コマンド（３．６．１５章）を参照し、エージェント名を変更する。
※エージェント名設定後、NQ の再起動が必要です。

９．４．１．２　IPアドレスを変更する手順

(1) IP アドレスを変更する

ネットワークインターフェース設定コマンド（３．６．７章）を参照し、該当 NQ の IP アドレスを変更する。

(2) NQ を再起動する

再起動コマンド（３．６．１３章）を参照し、NQ を再起動する。

９．４．２　集中管理モードの場合

９．４．２．１　エージェント名を変更する手順

(1) 不正接続防止、データ収集を停止する

DomainManager の集中管理画面の「エージェント管理」より該当 NQ の不正接続防止、データ収集を停止する。

(2) ホストデータをバックアップする

ホストエクスポートコマンドを使用し、ホストデータをバックアップする。

※ホストエクスポートコマンドについては、ドメインマネージャオンラインヘルプの「ホスト情報のエクスポートコマンドについて」を参照してください。

(3) エージェント名を変更する

エージェント名設定コマンド（３．６．１５章）を参照し、エージェント名を変更する。

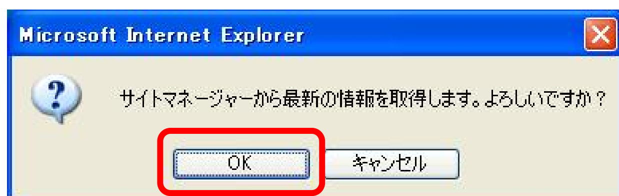
※エージェント名設定後、NQ の再起動が必要です。

(4) SiteManager の最新情報を取得する

NQ が起動したら、DomainManager 集中管理画面の「サイト管理」より SiteManager の最新情報を取得する。



このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



(5) エージェントの詳細設定を入力する

DomainManager 集中管理画面の「エージェント管理」にエージェント名変更後のエージェント情報が表示されたら、「エージェント管理詳細画面」よりエージェント名変更前の情報を入力してください。

(6) ホストデータをリストアする

DomainManager 集中管理画面の「エージェント管理」に IP アドレス変更後のエージェント情報が表示されたら、ホストインポートコマンドを使用してホストデータをリストアする。

※ホストインポートコマンドについては、ドメインマネージャオンラインヘルプの「ホスト情報のインポートコマンドについて」を参照してください。

(7) データ収集を開始する

DomainManager 集中管理画面の「エージェント管理」にエージェント名変更後のエージェント情報が表示されたらデータ収集を開始する。

(8) 不正接続防止を開始する

DomainManager 集中管理画面の「エージェント管理」より該当 NQ の不正接続防止を開始する。

(9) 古いエージェントを削除する

DomainManager 集中管理の「エージェント管理」より変更前のエージェント情報を削除する。



このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



９．４．２．２　IPアドレスを変更する手順

(1) 不正接続防止、データ収集を停止する

DomainManager の集中管理画面の「エージェント管理」より該当 NQ の不正接続防止、データ収集を停止する。

(2) NQ を停止する

エージェント停止コマンド（３．６．２５章）を参照し、該当 NQ のサービスを停止する。

(3) ホストデータをバックアップする

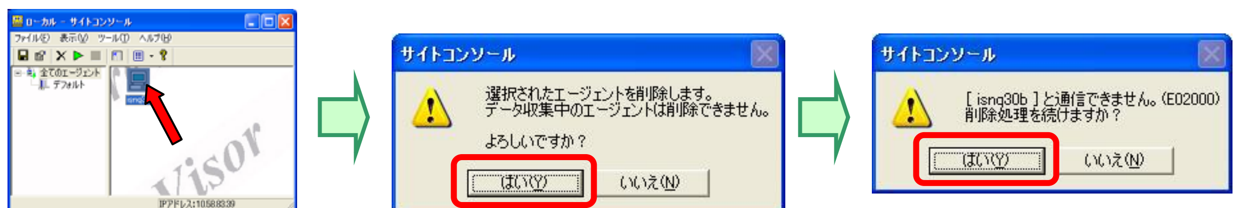
ホストエクスポートコマンドを使用し、ホストデータをバックアップする。

※ホストエクスポートコマンドについては、ドメインマネージャオンラインヘルプの「ホスト情報のエクスポートコマンドについて」を参照してください。

(4) エージェントを削除する

サイトコンソールを起動し、該当 NQ を削除する。

※NQ と通信できない旨のメッセージが表示されますが、そのまま削除してください。



(5) RCV ファイルを Backup フォルダへ移動する

DomainManager より該当 NQ を管理する SiteManager の最新 RCV ファイルを Backup フォルダへ移動する。

【RCV ファイル保存場所】

C:¥Program Files¥SecureVisor¥DomainManager¥RecvData¥AAA_BBB_YYYYMMDDHHMMSS.RCV ※DomainManager を "C:¥Program Files¥SecureVisor" にインストールした場合

※ AAA は、SiteManager の IP アドレス。
BBB は、サイト ID
YYYYMMDDHHMMSS は、日時
例：「192.168.0.100_001_20080824.RCV」

【異動先フォルダの場所】

C:¥Program Files¥SecureVisor¥DomainManager¥Backup¥AAA_BBB

※DomainManager を ″C:¥Program Files¥SecureVisor″ にインストールした場合

※ AAA は、SiteManager の IP アドレス。
BBB は、サイト ID
例：「192.168.0.100_001」

(6) IP アドレスを変更する

ネットワークインターフェース設定コマンド（３．６．７章）を参照し、該当 NQ の IP アドレスを変更する。

(7) NQ を再起動する

再起動コマンド（３．６．１３章）を参照し、NQ を再起動する。

(8) SiteManager の最新情報を取得する

NQ が起動したら、DomainManager 集中管理画面の「サイト管理」より SiteManager の最新情報を取得する。



このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



(9) ホストデータをリストアする

DomainManager 集中管理画面の「エージェント管理」に IP アドレス変更後のエージェント情報が表示されたら、ホストインポートコマンドを使用してホストデータをリストアする。
※ホストインポートコマンドについては、ドメインマネージャオンラインヘルプの「ホスト情報のインポートコマンドについて」を参照してください。

(10) データ収集を開始する

DomainManager 集中管理画面の「エージェント管理」に IP アドレス変更後のエージェント情報が表示されたらデータ収集を開始する。

(11) 不正接続防止を開始する

DomainManager 集中管理画面の「エージェント管理」より該当 NQ の不正接続防止を開始する。

９．５　USBメモリを使用したNQの設定内容の確認方法

(1) USB メモリに設定ファイルを作成する

USB メモリのルートフォルダに設定ファイルを作成してください。設定ファイルの作成方法は、２．２．２章～２．２．４章を参照してください。

(2) USB メモリを差込み、NQ を起動する

設定ファイルを保存した USB メモリを NQ 筐体へ接続してください。接続完了後、電源ケーブルを NQ 筐体およびコンセントへ差し込むことにより、自動起動します。

但し、NQ30a の初期出荷製品は、電源ケーブル接続による自動起動を行いません。NQ30a が自動起動しない場合、電源スイッチを押下してください。起動状態は、電源ランプの点灯状態から確認してください。

なお、USB メモリから設定ファイルを認識させることができるのは、起動時のみです。NQ の起動後に筐体へ USB メモリを接続しても、設定ファイルを認識させることはできませんので注意してください。

(3) USB メモリに作成されたテキストファイルで NQ の設定状態を確認する

起動から約 1 分経過後、NQ 筐体から USB メモリを取り外し、USB メモリを PC に接続してください。NQ が USB メモリを正常に認識できた場合(※1)は、USB メモリのルートフォルダにテキストファイル（svconflog.txt）が作成されます。このテキストファイルに NQ の設定状態が出力(※2)されていますので確認してください。

(※1)テキストファイルが作成されない場合、NQ と USB メモリの相性が悪い、NQ が暗号化 USB メモリに対応していない、NQ30c に USB2.0 以外の USB メモリが使用されているなどが原因で、認識できていない可能性があります。

(※2)エージェント設定確認コマンド（list na）（３．６．５章参照)、ネットワークインターフェース確認コマンド（list if）（３．６．３章参照)、ネットワークインターフェースのネゴシエーション設定確認コマンド（list ifspeed）（３．６．１８章参照)、｢DNS サーバアドレス、ドメイン名確認コマンド（list ns）（３．６．４章参照）の実行結果が出力されます。

９．６　Apple社製端末を監視対象にする場合の設定必須パラメータ

DHCPクライアントのApple社製端末が不正接続防止された場合、Apple社製端末がDHCPのIPアドレスを繰り返し要求してしまうため、DHCPのアドレスプールが枯渇してしまうことが

あります。本現象を回避するためには、「DisableBroadCastJamArp」を「1」に設定してください。「DisableBroadCastJamArp」については、「７．４　各環境共通の設定可能パラメータ」、「８．２　確認、および変更が可能な属性の詳細」を参照してください。

９．７　Linux系OS端末を監視対象にする場合の設定必須パラメータ

Linux系OS等、ARPエントリ更新のロックタイムが設定されているOSの場合、NQからの偽装ARPを受け付けないように動作し、不正接続防止が正常に行なわれないことがあります。ARPエントリの偽装を有効にするために「SendArpDelay」を設定してください。このパラメータの設定値をOSのロックタイムより長い秒数にすることでARPエントリの偽装が有効になります。「SendArpDelay」については、「７．４　各環境共通の設定可能パラメータ」、「８．２　確認、および変更が可能な属性の詳細」を参照してください。

９．８　携帯端末を監視対象にする場合の設定必須パラメータ

・Apple 社製の携帯端末の場合

「９．６　Apple社製端末を監視対象にする場合の設定必須パラメータ」に記載している設定を行なってください。

・Android 系の携帯端末の場合

「９．７　Linux系OS端末を監視対象にする場合の設定必須パラメータ」に記載している設定を行なってください。

１０．NQの交換手順

工場出荷時のNQは以下の通り、暫定的なバージョンのNetworkAgentがプリインストールされています。

製品名	製品型番	バージョン
InterSec/NQ30a	N8100-1110Q	2.2g
InterSec/NQ30b	N8100-1200Q	2.2h
	N8100-1300Q	3.1g
InterSec/NQ30c	N8100-1400Q	2.2

NQ 交換後、新しい NQ にインストールされている NetworkAgent のバージョンが古い場合は、SiteManager オンラインヘルプの、[SecureVisor]->[SecureVisor その他の機能]->[NetworkAgent 自動バージョンアップ機能]を参照してバージョンアップを行ってください。(※)
（※）InterSec/NQ30c の場合、工場出荷時の状態でも Ver3.8 に対する必要な設定が可能ですので、初期設定時にSiteManagerと通信するために必要な設定と、Ver3.8に対する必要な設定を実施するだけで、運用が開始できます。

NQ交換時は、必ずエージェント名、IPアドレスは同一のままで実施してください。また、運用モードにより手順が異なりますので、以下を参照し、利用する運用モードに応じた手順で実施してください。

なお、NQ交換後のエージェント名やIPアドレスを変更したい場合は９．４章を参照してください。

１０．１　分散管理モードの場合

(1) 故障したNQをネットワークから切り離す

(2) 不正接続防止機能、データ収集を停止する

(a) SiteManagerサービスを停止する

NQの接続先に設定されているSiteManagerサービスを以下の手順で停止する。

Windowsの[スタート]ボタン→（設定→）コントロールパネル→管理ツール→サービス → [SecureVisor SiteManager]を選択し、サービスを停止。

(b) SiteManagerの管理するエージェント設定を変更する

SiteManager が保持している NQ の属性ファイルを編集し、不正接続防止機能、データ収集が停止するよう設定変更を行う。

【NQ の属性ファイル保存場所】

C:¥Program Files¥SecureVisor¥SiteManager¥Data¥AgentList¥*xxxx*¥attribute.dat ※SiteManager を "C:¥Program Files¥SecureVisor" にインストールした場合

※ *xxxx* は、NQ のエージェント名。

attribute.dat ファイルをメモ帳などのエディタで開き、以下の変更を行う。

◆不正接続防止機能（JamStatus）

JamStatus: On	→	JamStatus: Off

◆データ収集

CollectOfPacket: On	→	CollectOfPacket: Off

※ SiteManager の属性ファイルは、文字コードを Shift-JIS、改行コードを<CR>+<LF>で作成されています。使用するテキストエディタの設定を確認の上、編集、保存を行ってください。なお、Windows 標準のメモ帳は前述の設定を満たしているため、問題なく使用できます。

(c) SiteManager のサービスを開始する

NQ の接続先に設定されている SiteManager サービスを以下の手順で開始する。

Windows の[スタート]ボタン→（設定→）コントロールパネル→管理ツール→サービス → [SecureVisor SiteManager]を選択し、サービスを開始。

(3) NQ をネットワークに接続する

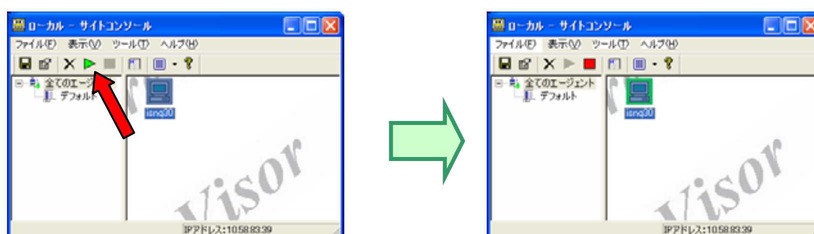
新しい NQ に交換前の NQ の初期設定を行った後、ネットワークに接続する。

(4) NQ が登録されたことを確認する

サイトコンソールを起動し、該当 NQ のエージェントが灰色の状態で登録されていることを確認する。

(5) データ収集を開始する

サイトコンソールを起動し、該当 NQ のデータ収集を開始する。

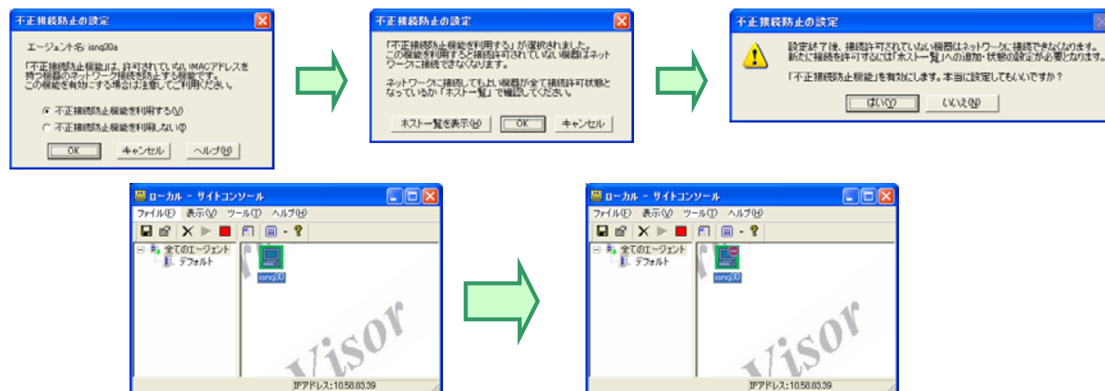


(6) 新NQが検知され、接続許可として登録されていることを確認する

ホスト一覧を起動し、新 NQ が「青」として登録されていない場合は、「青」に変更して保存する。

(7) 不正接続防止機能を開始する

サイトコンソールを起動し、[ファイル]-[不正接続防止の設定]から該当 NQ の不正接続防止機能を開始する。



１０．２　集中管理モードの場合

(1) 故障したNQをネットワークから切り離す

(2) 不正接続防止機能、データ収集を停止する

DomainManagerの集中管理画面から該当NQの不正接続防止機能、データ収集を停止する。

(a) 不正接続防止、およびデータ収集を停止する権限のあるユーザで集中管理機能にログインする。

(b) ［メニュー画面］で［エージェント管理］ボタンをクリックする。

(c) 表示された［メニュー ＞ エージェント管理］画面で［検索］ボタンをクリックする。

(d) 該当NQの［不正接続防止］の ▶ アイコンを２回クリックする。

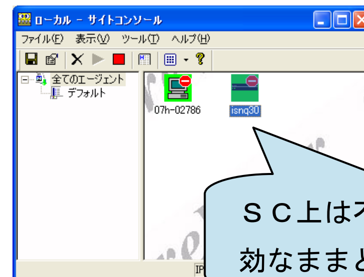
(e) 該当NQの［データ収集］の ▶ アイコンをクリックする

((d)(e)それぞれのアイコンが ■ に変わる)。

(f) 設定を反映させるため、[保存]ボタンをクリックする。



このとき、SiteManager のコンソール画面では、右図のような状態となります。



ＳＣ上は不正接続防止が有効なままとなります。

(3) NQ をネットワークに接続する

新しい NQ に交換前の NQ の初期設定を行った後、ネットワークに接続する。

(4) NQ が登録されたことを確認する

サイトコンソール上に、該当 NQ のエージェントが灰色の状態で登録されていることを確認する。

(5) データ収集を開始する

DomainManager の集中管理画面から該当 NQ のデータ収集を開始する。

(a) データ収集を開始する権限のあるユーザで集中管理機能にログインする。

(b) ［メニュー画面］で［エージェント管理］ボタンをクリックする。

(c) 表示された［メニュー ＞ エージェント管理］画面で［検索］ボタンをクリックする。

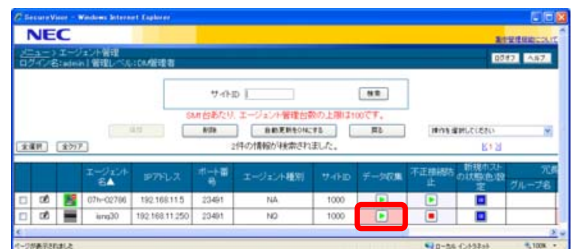
(d) 復旧した NQ［データ収集］の アイコンをクリックする

（アイコンが に変わる）。

(e) 設定を反映させるため、[保存]ボタンをクリックする。







(6) 新 NQ が検知され、接続許可として登録されていることを確認する

ホスト情報一覧を起動し、新 NQ が「青」として登録されていない場合は、「青」に変更して保存する。



(7) 不正接続防止機能を開始する

DomainManager の集中管理画面から該当 NQ の不正接続防止機能を開始する。

(a) 不正接続防止を開始する権限のあるユーザで集中管理機能にログインする。

(b) ［メニュー画面］で［エージェント管理］ボタンをクリックする。

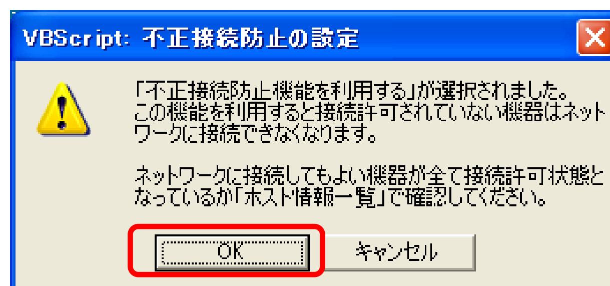
(c) 表示された［メニュー > エージェント管理］画面で［検索］ボタンをクリックする。

(d) 該当 NQ の［不正接続防止］の アイコンを２回クリックする（アイコンが に変わる）。

(e) 設定を反映させるため、[保存]ボタンをクリックする。



このとき、以下の確認ダイアログが表示されるので、[OK]を押してください。



１１．その他

１１．１　SecureVisorの最新情報

SecureVisor に関する最新情報は、下記のウェブサイトを参照してください。

http://www.nec.co.jp/cced/infocage/n_prevention/index.html

～以上～